Underrättelsetillsyns-
ombudsman

UNDERRÄTTELSETILLSYNS-OMBUDSMANNENS BERÄTTELSE FÖR ÅR 2020

B 10/2021 rd

UNDERRÄTTELSETILLSYNS-OMBUDSMANNENS BERÄTTELSE FÖR ÅR 2020

Innehåll

TILL RIKSDAGEN, RIKSDAGENS JUSTITIEOMBUDSMAN OCH STATSRÅDET

Detta är en berättelse om underrättelsetillsynsombudsmannens verksamhet under år 2020 till riksdagen, riksdagens justitieombudsman och statsrådet enligt 19 § 1 mom. i lagen om övervakning av underrättelseverksamheten.

I min första årsberättelse (B 14/2020 rd) inkluderade jag allmän information om vid den tiden nya former av underrättelsesystem och system för övervakning av underrättelseverksamhet. Jag upprepar inte denna information i denna årsberättelse. I likhet med den första årsberättelsen framför jag observationer om underrättelselagstiftningen även i denna årsberättelse. Jag hoppas fortfarande att mina observationer kan vara till nytta för den samhälleliga och professionella diskussionen om ämnesområdet som styr även min egen verksamhet. Ämnesområdet är i övrigt rätt långt sekretessbelagt.

Jag har haft tillgång till inrikesministeriets berättelse om användningen av underrättelseinhämtningsmetoder och skyddande av civil underrättelseinhämtning samt övervakningen av dem, försvarsministeriets berättelse om användningen av underrättelseinhämtningsmetoder och skyddande av militär underrättelseinhämtning samt övervakningen av dem, inrikesministeriets berättelse om användningen av hemliga informationsinhämtningsmetoder samt skyddande och övervakning av dem, Skyddspolisens berättelse om laglighetsövervakning samt årsberättelsen om den interna laglighetsövervakningen av den militära underrättelseinhämtningen för år 2020.

Helsingfors 27.4.2021

Kimmo Hakonen
underrättelsetillsynsombudsman

Etablering av underrättelsetillsynen

Underrättelsetillsynsombudsmannens första ofullständiga verksamhetsår 2019 och den första hälften av året för denna berättelse kan beskrivas som inledningsfasen för underrättelsetillsynen. Under den senare hälften av verksamhetsåret låg fokus på att etablera verksamheten.

Den extra personal som underrättelsetillsynsombudsmannafunktionen fått har gjort det möjligt att utvidga tillsynen. Övervakningen som underrättelsetillsynsombudsmannen utövar riktades i synnerhet i början mot proaktiv laglighetsövervakning, bland annat i form av juridiskt sakkunnigstöd gällande beredning av anvisningar och anordnande av utbildning på ett sätt som lämpar sig för ombudsmannens roll som extern laglighetsövervakare. Även laglighetsövervakning i realtid, dvs. granskning av underrättelsemyndigheternas tillståndskrav och beslut samt deltagande i domstolsbehandlingar som gäller metoder för underrättelseinhämtning har sedan början haft, och har fortfarande, en central roll. I takt med att underrättelseoperationer avancerat har det uppstått ett behov av – och tack vare den extra personal som underrättelsetillsynsombudsmannafunktionen fått – att även utöva laglighetsövervakning retroaktivt.

Å andra sidan, då underrättelsetillsynsombudsmannafunktionen fått extra personal, har man samtidigt behövt säkerställa den interna informationen. Underrättelsetillsynsombudsmannen, som verkar som ensam myndighet, ska få en övergripande helhetsbild av den verksamhet som övervakas.

Under verksamhetsåret började en verksamhetslokal som uppfyller höga informationssäkerhetskrav byggas för underrättelsetillsynsombudsmannen. Den nya verksamhetslokalen kommer att stå färdig nästa år.

Underrättelsetillsyns-ombudsmannafunktionen

Underrättelsetillsynsombudsmannafunktionen bildas av underrättelsetillsynsombudsmannen samt de föredragande och den övriga personalen.

Underrättelsetillsynsombudsmannen är i sin verksamhet självständig och oberoende, men han eller hon är administrativt placerad i anslutning till dataombudsmannens byrå. I praktiken innebär detta att underrättelsetillsynsombudsmannen får stöd i ärenden relaterade till administration och kommunikation av dataombudsmannens byrå. Underrättelsetillsynsombudsmannens dokumentförvaltning är dock av informationssäkerhetsskäl helt avskild från dataombudsmannens byrå.

I ett projekt tillsatt av justitieministeriet färdigställdes under verksamhetsåret en utredning om omorganisering av stöd- och administrationsuppgifter hos specialmyndigheter verksamma inom justitieministeriets förvaltningsområde. Ifall omorganiseringen av stöd- och administrationsuppgifter genomförs, omfattar den också det stöd i ärenden relaterade till administration och kommunikation som underrättelsetillsynsombudsmannafunktionen i nuläget får av dataombudsmannens byrå.

Personal

Underrättelsetillsynsombudsmannafunktionens resursbehov har i fråga om både volym och kvalitet ett samband med den takt som metoder för underrättelseinhämtning tas i bruk.

En administrativ medarbetare började arbeta 1.7.2020 och en specialsakkunnig 1.8.2020 inom underrättelsetillsynsombudsmannafunktionen. Den administrativa medarbetaren deltar även i övervakningsverksamheten vid sidan av sina administrativa uppgifter. Den specialsakkunniga fokuserar på övervakning av civil underrättelseinhämtning.

Ekonomi

Omkostnaderna för underrättelsetillsynsombudsmannafunktionen finansieras ur moment 25.01.03 (Omkostnader för myndigheter som verkar i anslutning till justitieministeriet) i statsbudgetens huvudtitel för justitieministeriets förvaltningsområde. Under verksamhetsåret var anslaget för underrättelsetillsynsombudsmannafunktionen 350 000 euro. Dessutom omfattade anslaget för dataombudsmannens byrå också kostnaderna för underrättelsetillsynsombudsmannafunktionens lokaler.

Enligt verksamhetsårets bokslut var underrättelsetillsynsombudsmannafunktionens omkostnader 203 000 euro. De oanvända delarna av anslagen för åren 2019 och 2020 överfördes till år 2021.

Kommunikation

Underrättelsetillsynsombudsmannafunktionen har en webbplats på finska, svenska och engelska på adressen tiedusteluvalvonta.fi. På webbplatsen publiceras underrättelseombudsmannens kolumner,

som ur olika perspektiv beskriver de juridiska ramarna av underrättelseverksamheten och övervakningen av den.

Underrättelsetillsynsombudsmannafunktionen har också ett Twitter-konto (@tiedusteluvalv), vars huvudsakliga syfte är att dirigera personer som är intresserade av aktuella frågor inom övervakningen av underrättelseverksamhet till funktionens webbplats.

Samarbete med intressentgrupper

Underrättelsetillsynsombudsmannafunktionens resursbehov påverkas i fråga om både volym och kvalitet även av samarbetsmöjligheter med andra instanser som övervakar underrättelseverksamheten. I fråga om kvalitativa resursbehov kan detta innebära till exempel anskaffning av informations- och kommunikationsteknisk expertis som är oberoende av underrättelsemyndigheterna via samarbetsarrangemang. Samarbetsarrangemangen kan möjliggöra tillgång till mångsidig sakkunskap på ett kostnadseffektivt sätt.

I synnerhet när det gäller retroaktiv laglighetsövervakning av underrättelseverksamheten är underrättelsetillsynsombudsmannens centrala samarbetspartner underrättelsemyndigheternas interna laglighetsövervakare. Den laglighetsövervakning som underrättelsetillsynsombudsmannen utövar retroaktivt är i stor utsträckning övervakning av den inre övervakningen som ombudsmannen fått kännedom om via granskningsberättelser från underrättelsemyndigheternas interna laglighetsövervakare. Dessutom utövar ombudsmannen sin egen retroaktiva laglighetsövervakning med fokus på olika teman. Ett tema är till exempel övervakning av granskningen av material som inhämtats genom underrättelse. Underrättelsetillsynsombudsmannen kan ge de interna laglighetsövervakarna och operativa juristerna hos underrättelsemyndigheterna juridiskt sakkunnigstöd på ett sätt som lämpar sig för ombudsmannens roll som extern laglighetsövervakare.

Även dataombudsmannen, i praktiken endera av de biträdande dataombudsmännen, är en central samarbetspartner för underrättelsetillsynsombudsmannen. När det gäller övervakning av användningen av underrättelseinformation är underrättelsetillsynsombudsmannens och dataombudsmannens uppgifter parallella, men övervakningen som de utför riktas på grund av olika övervakningsbefogenheter mot olika skeden av informationshanteringsprocessen: övervakningen som underrättelsetillsynsombudsmannen utför mot inhämtande av information med hjälp av metoder för underrättelseinhämtning och övervakningen som dataombudsmannen utför mot lagring av underrättelseinformation i register och behandlingen av information som lagrats i register.

Övervakningen av informationsutbyte gällande internationellt underrättelsesamarbete utgör ett specialområde. Det nationella intresset hos stater som deltar i internationellt underrättelsesamarbete, vilket ska beaktas vid informationsutbyte och dess övervakning, kan variera beroende på vilken typ av underrättelseföremål det är frågan om.

Underrättelseövervakarna samarbetar på internationell, europeisk och nordisk nivå. På grund av coronaviruspandemin arrangerades inga internationella möten för underrättelseövervakarna under verksamhetsåret.

Information om underrättelsetillsyns-ombudsmannens verksamhet

Coronaviruspandemin och de rådande undantagsförhållandena, som i övrigt präglade verksamhetsåret, påverkade inte genomförandet av själva tillsynen.

Utöver olika slags studiebesök gjorde underrättelsetillsynsombudsmannafunktionen under verksamhetsåret 172 ordinarie inspektionsbesök under vilka underrättelsemyndigheters samtliga beslut om användning av underrättelseinhämtningsmetoder och skyddande av underrättelseinhämtning granskades. Informationen om antalet beslut är sekretessbelagd på basis av 24 § 1 mom. 5, 9 och 10 punkten i offentlighetslagen.

Dessutom deltog underrättelsetillsynsombudsmannafunktionen i alla sammanträden om underrättelseinhämtningsmetoder vid Helsingfors tingsrätt. Informationen om antalet behandlade ärenden är sekretessbelagd på basis av 5 § 2 mom. i lagen om offentlighet vid rättegång i allmänna domstolar.

Under verksamhetsåret mottog ombudsmannen 20 skrivelser som främst kan tolkas som utredningsbegäranden. Utöver dessa inkom inga skrivelser som kan tolkas som klagomål. I Finland används inget egentligt visselblåsarsystem för civil och militär underrättelseinhämtning, men utöver utredningsbegäranden och klagomål kan tips lämnas till underrättelsetillsynsombudsmannen om eventuella missförhållanden i underrättelseverksamhet konfidentiellt och även anonymt.

Metoderna för övervakningen av underrättelseverksamhet samt klagomåls- och utredningsbegäransärendena och mottagande av tips är i regel sekretessbelagda i syfte att säkerställa underrättelsetillsynens effektivitet och skydda dem som anför klagomål eller lämnar in utredningsbegäranden eller tips (se 24 § 1 mom. 6 och 15 punkten i offentlighetslagen när det gäller allmän offentlighet och 11 § 2 mom. 1 punkten när det gäller övervakningsobjektets rätt att få information). På grund av underrättelseverksamhetens känsliga karaktär kunde offentliggörandet av anförande av klagomål och utredningsbegäranden och lämnande av tips minska personers villighet att inleda ärenden och tipslämnarnas villighet att lämna tips och således äventyra underrättelsetillsynsombudsmannens tillgång till information (jfr skydd för rapportörers identitet i dataskyddsärenden). När det gäller underrättelseverksamhet har även föremålen för underrättelseinhämtningsmetoder

endast begränsad rätt till insyn med stöd av specialbestämmelser i underrättelselagarna. Detta begränsar underrättelsetillsynsombudsmannens möjligheter att informera personer som lämnat in begäranden om utredning om de eventuellt varit föremål för underrättelseinhämtningsmetoder.

Under verksamhetsåret blev det inte aktuellt att framföra klagan över Helsingfors tingsrätts beslut, meddela förordnanden om avbrytande eller avslutande av underrättelseinhämtningsmetoder, anmäla underrättelsemyndigheters förfarande till förundersökning eller ge en anmärkning till underrättelsemyndigheter.

Särskilt betydelsefulla med tanke på övervakningen av underrättelseverksamhetens lagenlighet är de helt nya befogenheterna för hemlig informationsinhämtning som blivit tillgängliga för underrättelsemyndigheterna i och med att underrättelselagarna trädde i kraft. Om dessa finns det ingen tidigare erfarenhet i fråga om kriminalunderrättelseverksamhet. Av denna anledning tog underrättelsetillsynsombudsmannen på eget initiativ för bedömning sådana lagtolkningsfrågor som gällde ett sådant beslut gällande befogenheter av en underrättelsemyndighet, som kunde ha en allmännare betydelse än det aktuella, enskilda beslutet. Det rörde sig bland annat om relationen mellan civil och militär underrättelseinhämtning och brottsbekämpning, som behandlas närmare nedan. Efter att ha begärt och fått utredningar av underrättelsemyndigheten delgav underrättelsetillsynsombudsmannen underrättelsemyndigheten sina synpunkter gällande lagtolkningsfrågorna.

Användningen av metoder för underrättelseinhämtning som underrättelsetillsynsombudsmannen granskade riktades under verksamhetsåret mot verksamhet som ska anses utgöra ett allvarligt hot mot den nationella säkerheten.

Under verksamhetsåret hördes underrättelsetillsynsombudsmannen tre gånger av riksdagens underrättelsetillsynsutskott. Ombudsmannen gav två utlåtanden till riksdagens förvaltningsutskott och två utlåtanden till justitieministeriet gällande författningsprojekt. Dessutom gav ombudsmannen inrikesministeriet och försvarsministeriet utlåtanden som gällde beredningen av utredningar om hur underrättelselagstiftningen fungerar.

Underrättelsetillsyns-ombudsmannens iakttagelser av lagstiftningen

Nedan presenteras vissa iakttagelser om de rättsliga ramarna för civil och militär underrättelseinhämtning. De anknyter inte nödvändigtvis till konkreta, i praktiken förekommande lagtolkningssituationer.

Iakttagelserna gäller särskilt skillnaderna mellan civil och militär underrättelseinhämtning och kriminalunderrättelseverksamhet.

Syftet med informationsinhämtning

Underrättelseverksamhet är hemligt inhämtande av information. Inhämtande av information är inte ett självändamål.

Med kriminalunderrättelseverksamhet stöds förebyggande, avslöjande eller utredning av brott. Med förebyggande av brott avses åtgärder som syftar till att förhindra ett brott eller avbryta ett redan påbörjat brott och begränsa den direkta skada eller fara som brottet medför. Med avslöjande av brott avses åtgärder som syftar till att klarlägga om det finns en i förundersökningslagen avsedd grund för inledande av förundersökning.

Civil och militär underrättelseinhämtning stöder civila och militära underrättelsemyndigheters verksamhet för att skydda den nationella säkerheten, den högsta statsledningens säkerhetspolitiska beslutsfattande och andra myndigheters verksamhet som anknyter till den nationella säkerheten. Civila och militära underrättelsemyndigheters verksamhet för att skydda den nationella säkerheten kan vara egentlig påverkan eller till exempel utarbetande av säkerhetsutredningar. Andra myndigheters verksamhet som anknyter till den nationella säkerheten kan vara egentlig påverkan eller någon annan verksamhet. Civila och militära underrättelsemyndigheter kan stödja andra myndigheters övriga verksamhet genom att till exempel ge dem utlåtanden. Då civil och militär underrättelseinhämtning till sin grundläggande karaktär handlar om att kombinera osäkra uppgifter och svaga signaler, kan okontrollerad underrättelseinformation inte användas som sådan i beslutsfattande som påverkar individers rättigheter eller skyldigheter.

Föremål för informationsinhämtning

Vid kriminalunderrättelseverksamhet är föremålen för informationsinhämtning sådana planerade eller redan utförda gärningar som enligt strafflagen eller andra lagar är straffbara.

Föremålet för informationsinhämtning vid civil och militär underrättelseinhämtning är verksamhet som allvarligt hotar den nationella säkerheten enligt polislagens kapitel om civil underrättelseinhämtning, lagen om civil underrättelseinhämtning avseende datatrafik och lagen om militär underrättelseverksamhet. När det gäller militär underrättelseverksamhet föreskrivs utöver om föremål för underrättelseinhämtning även om fastställandet av underrättelseuppdrag, som är mer exakta. Då föremålen för civil och militär underrättelseinhämtning samt inriktning av informationsinhämtning och inriktning av åtgärder för informationsinhämtning, vilka behandlas nedan, inte är lika strikt reglerade som i kriminalunderrättelseverksamhet, betonas vid användningen av befogenheter för informationsinhämtning vid civil och militär underrättelseinhämtning och övervakningen av deras användning betydelsen av bedömningen av allvarsgraden i det hot mot den nationella säkerheten som den verksamhet som är föremål för informationsinhämtning utgör.

Föremålet för informationsinhämtning är i fråga om operativ civil underrättelseinhämtning, operativt civilt kontraspionage och operativt militärt kontraspionage, som stöder den nationella säkerheten, är verksamhet vars delgärningar skulle uppfylla rekvisitet för landsförräderi, högförräderi eller terroristbrott när de avancerat till brottsstadiet. När det gäller strategisk civil underrättelseinhämtning och strategisk militär underrättelseinhämtning som stöder den högsta statsledningens beslutsfattande samt operativ militär underrättelseinhämtning som stöder den nationella säkerheten kan föremålet för informationsinhämtning också vara någon annan än en straffbar eller i övrigt lagstridig verksamhet, om den dock allvarligt hotar den nationella säkerheten.

Om operativa informationsinhämtningsmetoder används för att skaffa information som behövs vid strategisk civil och militär underrättelseinhämtning, ska man i tillståndskraven och besluten som gäller användningen av metoder för underrättelseinhämtning specificera den konkreta verksamhet som är föremål för informationsinhämtningen som grund för bedömningen av uppfyllandet av förutsättningar för användningen av metoden för underrättelseinhämtning, även om produkten av informationsinhämtningen, dvs. den strategiska hotanalysen, skulle ha en mer abstrakt karaktär.

Så kallad stormningsobservation för ett säkert genomförande av en myndighetsåtgärd och den delvis snarlika taktiska militära underrättelseinhämtning som genomförs i självskyddssyfte är ett kapitel för sig. I samband med stormningsobservation jämställs grunden för ingripande i hemligheten i fråga om förtroliga meddelanden med den i grundlagen nämnda säkerhetskontrollen snarare än med brottsutredning eller med informationsinhämtning gällande verksamhet som hotar den nationella säkerheten (GruU 36/2017 rd). Det föreskrivs särskilt om att skydda underrättelsetjänstemannens och informationskällans säkerhet genom att förse honom eller henne med en teknisk anordning som möjliggör avlyssning och observation.

I en del av föremålen för civil och militär underrättelseinhämtning är aktören alltid en främmande stat. I en del av föremålen kan aktören också vara någon annan instans.

En främmande stats militära verksamhet utgör notoriskt ett allvarligt hot mot den nationella säkerheten i den stat som är föremål för verksamheten och en främmande stats övriga fientliga verksamhet utgör i allmänhet allvarligt hot mot den nationella säkerheten i den stat som är föremål för verksamheten. Förutom främmande stater kan snarast aktörer som terroristiska och kriminella organisationer ha förmågan att utgöra ett allvarligt hot mot den nationella säkerheten i målstaten. Ett allvarligt hot mot den nationella säkerheten förknippas i fråga om både främmande stater och terroristiska och kriminella organisationer med hur planmässig, organiserad, professionell och fortlöpande eller upprepad deras verksamhet är samt med vilka resurser de har tillgängliga. Det är frågan om aktörer som förmår att i extrema fall genomföra ett väpnat angrepp eller annat så allvarligt angrepp att det kan jämställas med ett väpnat angrepp. När det gäller kriminalunderrättelseverksamhet är föremålen snarlika i fråga om bekämpning av organiserad brottslighet och terrorism. Professionaliteten och kontinuiteten i den verksamhet som är föremål för informationsinhämtning är av betydelse även för skyddet och sekretessen vid informationsinhämtning samt förhållandet mellan civil och militär underrättelseinhämtning och brottsbekämpning, vilka behandlas nedan.

Huruvida föremålet för civil och militär underrättelseinhämtning är en statlig eller någon annan aktör är av betydelse för förutsättningarna för användningen av metoder för underrättelseinhämtning och skyldigheten att informera föremålet för informationsinhämtningen om att metoden för underrättelseinhämtning används. Förutsättningen för användningen av metoder för underrättelseinhämtning är i fråga om statliga aktörer att användningen är behövlig och i fråga om andra aktörer att användningen är nödvändig för utförandet av ett underrättelseuppdrag. Det föreligger ingen skyldighet att informera statliga aktörer som är föremål för underrättelseinhämtning om att en metod för underrättelseinhämtning används, medan det i regel finns en sådan skyldighet i fråga om andra aktörer.

Med en statlig aktör avses en myndighet i en främmande stat eller en med en sådan jämställbar aktör samt den som är i dennes tjänst eller lyder under eller styrs av denne. De som är i en tjänst i en myndighet i en främmande stat är bland annat underrättelsetjänstemän och de som styrs av en myndighet i en främmande stat är bland annat dess styrda informationskällor. Det kan också röra sig om så kallade proxyaktörer eller suppleant som verkar för en främmande stats räkning eller med en främmande stats samtycke. En myndighet i en främmande stat kan också ha samarbetspartner bland sådana individer eller sammanslutningar vars relation till myndigheten är vagare än en egentlig bestämmanderätts- eller styrningsrelation som skapar ställningen som en statlig aktör. Samarbetspartnerna bistår emellertid myndigheterna i den främmande staten i verksamhet som hotar den nationella säkerheten i staten som är föremål för verksamheten eller bidrar till denna verksamhet. En person som är i tjänst i myndighet i en främmande stat kan också åtnjuta diplomatisk immunitet, som påverkar det faktiska fullgörandet av straffansvaret.

En främmande stat är en privaträttslig juridisk person, men i samband med avvärjande av en främmande stats militära eller fientliga verksamhet ska statens och dess representanters verksamhet bedömas via statens ställning som subjekt inom internationellt rätt. Bestämmelser om avvärjande av en främmande stats fientliga

verksamhet finns i territorialövervakningslagen. Enligt territorialövervakningslagen är fientlig verksamhet utöver territoriekränkningar även spaning och elektronisk störning som riktas mot objekt som är viktiga med tanke på den nationella säkerheten. I samband med en främmande stats väpnade angrepp eller ett därmed jämförbart angrepp betonas perspektivet för avvärjande av angrepp i stället för perspektivet för brottsbekämpning. Bestämmelser om avvärjande av ett väpnat angrepp eller ett motsvarande yttre hot finns i lagen om försvarsmakten. Vid ett väpnat angrepp eller annat så allvarligt angrepp att det kan jämställas med ett väpnat angrepp är det frågan om undantagsförhållanden enligt beredskapslagen. I beredskapslagen finns bestämmelser om bland annat åtgärder för att avvärja kränkningar av dataskyddet.

Subjektet i internationell humanitär rätt, dvs. rättsreglerna för krig, kan också vara en terroristorganisation. Bestämmelserna om terroristbrott, landsförräderibrott, högförräderibrott samt aggressionsbrott och krigsförbrytelser och brott mot mänskligheten kan beroende på perspektivet tillämpas på delvis likartade fall.

Befogenheter för informationsinhämtning

Befogenheterna för informationsinhämtning vid civil och militär underrättelseinhämtning är i huvudsak liknande som vid kriminalunderrättelseverksamhet. Kontrollerade leveranser, som är tillgängligt vid kriminalunderrättelseverksamhet, kan dock inte användas vid civil och militär underrättelseinhämtning (se dock underlåtenhet att ingripa i brott i samband med förhållandet mellan civil och militär underrättelseinhämtning samt brottsbekämpning nedan). Vid kriminalunderrättelseverksamhet kan man åter inte använda platsspecifik underrättelseinhämtning, kopiering, kopiering av försändelser, kvarhållande av försändelser för kopiering eller underrättelseinhämtning som avser datatrafik, vilka kan användas vid civil och militär underrättelseinhämtning, eller radiosignalspaning eller underrättelseinhämtning som avser utländska datasystem, vilka kan användas vid militär underrättelseinhämtning. Vid behandling av tekniska data är det frågan om befogenhet gällande inriktning av underrättelseinhämtning som avser datatrafik som föregår underrättelseinhämtning som avser datatrafik.

Till skillnad från kriminalunderrättelseverksamhet anses användning av informationskällor vid civil och militär underrättelseinhämtning inte vara en egentlig befogenhet för informationsinhämtning. Elementär observation anses inte kräva en egentlig befogenhetsbestämmelse vid kriminalunderrättelseverksamhet eller civil och militär underrättelseinhämtning.

Elektronisk kommunikation utgör en tämligen komplex verksamhetsmiljö för regleringen av befogenheter för informationsinhämtning både kriminalunderrättelseverksamhet samt civil och militär underrättelseinhämtning och för hur ställningen för aktörer som anknyter till informationsinhämtningen bestäms. I och med den snabba utvecklingen inom kommunikationsteknik och servicekoncept inom elektronisk kommunikation som utnyttjar den kan det finnas utrymme för tolkning även i grundläggande begrepp inom elektronisk kommunikation, såsom förtroligt meddelande och kommunikation, kommunikationsnät, kommunikationsförmedlare och kommunikationstjänst. Det kan vara krävande att samordna regleringen gällande tillhandahållande av elektroniska kommunikationstjänster och regleringen om hemlig

informationsinhämtning avseende elektronisk kommunikation också på grund av de olika syftena och målen med regleringen. Dessutom kan bestämmelser som gjorts upp vid olika tider använda olika termer för samma eller nästan samma begrepp och samma termer kan användas för delvis olika begrepp (till exempel identifierings-, förmedlings- eller trafikuppgift och lokaliserings- eller lägesuppgift). Det faktiska betydelseinnehållet i begreppen kan också ha förändrats på grund av den tekniska utvecklingen.

Elektronisk kommunikation är telekommunikation eller radiokommunikation. För telekommunikation används kommunikationsnät och för radiokommunikations används radioförbindelser, som är avskild från kommunikationsnäten. I kommunikationsnät kan det förutom delar som är uppbyggda av metalledare eller optiska fibrer också finnas delar som är uppbyggda med hjälp av radioförbindelser (till exempel radiolänkförbindelser i det allmänna kommunikationsnätet, förbindelser mellan terminalen och basstationen i ett mobilnät, förbindelser mellan terminalenhet och trådlöst lokalt nätverk samt Bluetooth-förbindelser ett personligt nätverk). En mobil enhet kan samtidigt vara en mobilterminal i mobilnätet, en dator ansluten till ett lokalt nätverk och en radiomottagare i ett positioneringssystem. En radioförbindelse kan också skapas med hjälp av en satellit belägen i rymden ovanför staters luftrum. Radioförbindelser som skapats med hjälp av en satellit kan utnyttjas i satellittelefonnät (någon annan kommunikationsförbindelse som nämns separat i bestämmelsen om teleavlyssning i lagen om militär underrättelseverksamhet) och satellitpositioneringssystem.

Kommunikationsnät och radioförbindelser som är avskilda från kommunikationsnät används för att förmedla förtroliga röst-, text-, bild- och datameddelanden mellan fysiska personer, men även till exempel meddelanden som är avsedda för allmänheten, meddelanden gällande användning av informationssystem anslutna till kommunikationsnätet eller tjänster som tillhandahålls på internet samt meddelanden som innehåller lägesuppgifter gällande tekniska enheters funktion och kommandon som används för att styra enheterna.

Grunden för regleringen av informationsinhämtning avseende telekommunikation härrör från tidsperioden för traditionella telefonnät. Under tidsperioden för moderna och ständigt avancerande datakommunikationsnät bildas ramarna för telekommunikation av kommunikationsnät som är anslutna till varandra och deras teleterminal- och nätverksutrustning samt olika lager i dataöverföring gällande förmedling av meddelanden. Djupet och bredden av ingripandet i hemligheten i förtroliga meddelanden och annat skydd för privatliv för personer som är föremål för informationsinhämtning och utomstående vid utövandet av informationsinhämtningsbefogenheter samt den rättsliga karaktären av de befogenheter som används vid informationsinhämtning kan variera beroende på vilken del av näthelheten och vilken slags information informationsinhämtningsåtgärderna riktas mot. Huruvida den inhämtade informationen kan förens med en fysisk eller juridisk person kan bero på vilket lager av dataöverföringen som är föremål för informationsinhämtning.

En myndighet behöver en lagstadgad befogenhet för att inhämta och utnyttja information som ingriper i en fysisk persons grundläggande fri- och rättigheter eller som i regel är förbjuden enligt lag och eventuellt föreskrivits som straffbar. Även en person som fungerar som representant för en främmande stat eller medlem i en terroristgrupp eller organiserad kriminell grupp åtnjuter i sig

skydd för de grundläggande fri- och rättigheterna, men i personens verksamhet av detta slag är det inte frågan om personens privatliv och personliga omständigheter i den mest genuina betydelsen av dessa begrepp. Bland annat är olovlig avlyssning och olovlig observation straffbart. En kriminalunderrättelsemyndighet samt civil och militär underrättelsemyndighet behöver befogenheter också för att göra observationer som kan förenas med en fysisk person om öppen verksamhet, om det är frågan om något annat än kortvarig observation. Vid annan än kortvarig observation är det frågan om systematisk observation. Det föreskrivs särskilt om teknisk övervakning av på förhand ospecificerade personer på en allmän plats eller allmän väg eller i samband med tull-, gräns- eller territorialövervakning.

Enligt grundlagen är hemligheten i fråga om förtroliga meddelanden okränkbar. På de grunder som anges i grundlagen kan det dock föreskrivas om nödvändiga begränsningar i meddelandehemligheten. Bestämmelserna om kommunikationens konfidentialitet och integritetsskydd i lagen om tjänster inom elektronisk kommunikation tillämpas på förtroliga meddelanden mellan fysiska personer, men även på övriga telemeddelanden och radiosändningar. I samband med såväl förtroliga telemeddelanden och radiosändningar som andra telemeddelanden och radiosändningar kan det röjas uppgifter som omfattas av personens skydd för privatliv, som tryggas i grundlagen. Exempel på sådana uppgifter är uppgifter om personens levnadssätt, fritidssysselsättningar och andra personliga förhållanden.

Orättmätigt inhämtande av innehållet eller identifieringsuppgifterna i ett telemeddelande som förmedlas via kommunikationsnätet uppfyller brottsrekvisitet för kränkning av kommunikationshemlighet. Enligt lagen om tjänster inom elektronisk kommunikation får den som har tagit emot eller annars fått kännedom om ett telemeddelande, radiokommunikation, identifieringsuppgifter eller lokaliseringsuppgifter som inte är avsedda för honom eller henne, inte utan samtycke av en kommunikationspart eller den som ska lokaliseras röja eller utnyttja meddelandets innehåll, identifierings- eller lokaliseringsuppgifter eller uppgifterna om meddelandets eller lokaliseringsuppgifternas existens, om inte något annat föreskrivs i lag. Brott mot förbudet uppfyller rekvisitet för sekretessbrott.

Uppgifter som gäller telekommunikation kan inhämtas i allmänna kommunikationsnät som teleföretag använder eller kommunikationsnät med ett begränsat antal användare som företag och andra organisationer som fungerar som sammanslutningsabonnenter använder eller i teleterminalutrustning. När information inhämtas hos teleföretag eller sammanslutningsabonnenter kan det vara fråga om teleavlyssning eller inhämtande av information i stället för teleavlyssning (telemeddelandets innehåll) eller teleövervakning (telemeddelandets identifieringsuppgifter och teleadressens eller teleterminalutrustningens lokaliseringsuppgifter som fås från kommunikationsnätet). Teleavlyssning och teleövervakning kan också genomföras med myndighetens tekniska anordningar. Teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning inriktas på teleadressen eller teleterminalutrustningen. Förutom teleterminalutrustning kan även nätverksutrustning ha en teleadress. I stället för teleterminalutrustning kan nätverksutrustning kopplas till en teleanslutning i det allmänna kommunikationsnätet. I detta fall bildas ett lokalt eller personligt nätverk med en begränsad användarkrets mellan teleanslutning-

en och teleterminalutrustningen. När information om meddelandets innehåll inhämtas ur en personlig teknisk anordning som lämpar sig för sändning och mottagning av meddelanden och finns i direkt anslutning till teleterminalutrustningen eller ur förbindelsen mellan en sådan anordning och teleterminalutrustningen är det fråga om inhämtande av information i stället för teleavlyssning. När information om innehållet eller identifieringsuppgifterna i sådana telemeddelanden som ännu inte eller inte längre förmedlas i kommunikationsnätet inhämtas ur teleterminalutrustningen, är det fråga om teknisk observation av utrustning.

Sådana tekniska anordningar som är kombinationer av teleterminalutrustning eller nätverksutrustning och en dator kan anslutas till kommunikationsnätet. I detta fall används kombinationsutrustningens teleterminalutrustningsdel för sändning, behandling och mottagning av meddelanden och kombinationsutrustningens nätverksutrustningsdel för överföring eller styrning av meddelanden i kommunikationsnätet. Datorerna kan vara till exempel arbetsstationer eller ha rollen som olika slags servrar. Lagrings- eller annan serverkapacitet kan också skaffas hos leverantörer av utlagda molntjänster och serverhotelltjänster. Även när information inhämtas ur kombinationsutrustningens datordel kan det vara fråga om teknisk observation av utrustning (observation av en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara).

Tekniska anordningar som anslutits till kommunikationsnätet kan även vara kombinationer av teleterminalutrustning och en avlyssnings- eller visningsanordning eller en radiomottagare som fungerar som positioneringsanordning i ett satellit- eller annat radiopositioneringssystem. I detta fall kan ljudet, bilden eller informationen om anordningens position som avlyssnings-, visnings- eller positioneringsanordningsdelen producerar förmedlas via kommunikationsnätet med hjälp av kombinationsutrustningens teleterminalutrustningsdel. Det kan också vara fråga om sådan kombinationsutrustning som består av terminalutrustning och en positioneringsanordning som inte kan användas för sändning och mottagning av meddelanden, dvs. vars terminalutrustningsdel inte är teleterminalutrustning. När information inhämtas ur avlyssnings-, visnings- eller positioneringsanordningsdelen i kombinationsutrustning kan det vara fråga om teknisk avlyssning (avlyssning av en persons samtal eller meddelande som inte är avsett för utomstående med hjälp av en teknisk anordning, metod eller programvara), optisk observation (iakttagande av en person eller ett utrymme eller någon annan plats med en kamera eller andra utplacerade tekniska anordningar, metoder eller programvaror) eller teknisk spårning (spårning av förflyttning av föremål, ämnen eller egendom med hjälp av radiosändare som fästs eller som redan finns på objektet eller med hjälp av någon annan liknande teknisk anordning, metod eller programvara).

På informationsinhämtning som gäller innehållet eller identifieringsuppgifterna i en konfidentiell radiosändning (radiostationens beteckning, typen av radiosändare eller radiosändningens begynnelsetidpunkt, längd eller sändningsplats) torde man kunna tillämpa bestämmelserna om teknisk avlyssning (avlyssning av samtal eller meddelande som inte är avsett för utomstående med hjälp av en teknisk anordning i syfte att ta reda på innehållet i samtalet eller meddelandet eller utreda deltagarnas verksamhet), även om typfallen för teknisk avlyssning är annorlunda. Spårning av förflyttningen av en radiosändare eller någon annan teknisk anordning som avger elektromagnetisk strålning

kan vara teknisk spårning baserad på radiopositionering. Det kan till exempel vara fråga om en radiosändare som fungerar som en spårningsanordning. Dessutom kan man i samband med till exempel observation utan separata befogenheter göra yttre observationer om en radiosändares eller annan teknisk anordnings funktion som avger elektromagnetisk strålning men som inte anknyter till konfidentiella radiosändningar. Det kan till exempel vara frågan om en radar eller störsändare. När en teknisk anordnings funktion observeras inifrån anordningen är det fråga om teknisk observation av utrustning.

Lagen om tjänster inom elektronisk kommunikation tillämpas förutom på tillhandahållande av till kommunikationsförmedling relaterade nättjänster och kommunikationstjänster även på tillhandahållande av mervärdestjänster. Mervärdestjänsterna baserar sig på behandling av identifieringsuppgifter för meddelanden eller lokaliseringsuppgifter för abonnemang eller terminaler i kommunikationsnätet för andra ändamål än för att förmedla meddelande. Identifieringsuppgifter för meddelande anknyter till förmedlingen av ett enskilt meddelande och de innehåller även den aktuella kommunikationshändelsens uppgifter från kommunikationsnätet om teleabonnemangets eller teleterminalutrustningens läge. Uppgifter om ett mobilabonnemangs eller en mobilterminalutrustnings läge fås i detta fall med hjälp av basstationspositionering. Lokaliseringsuppgifter för mobilabonnemanget eller mobilterminalutrustningen som inte hör samman med förmedling av meddelanden kan däremot basera sig på basstationspositionering eller satellit- eller annan radiopositionering. Lokaliseringsuppgifter som baserar sig på basstationspositionering av mobilabonnemanget eller mobilterminalutrustningen hör samman med upprätthållande av beredskap för förmedling av meddelanden och de fås från kommunikationsnätet. Lokaliseringsuppgifter som baserar sig på satellit- eller annan radiopositionering av mobilabonnemanget eller mobilterminalutrustningen fås från terminalutrustningen och kan förmedlas via kommunikationsnätet.

I samband med mervärdestjänster kan frågan beträffande omfattningen på rätten att få information som gäller kunduppgifter för kriminalunderrättelsemyndigheter och civila och militära underrättelsemyndigheter aktualiseras. Detta behandlas nedan i samband med befogenheter avseende information. När det gäller civil och militär underrättelseinhämtning kan det i detta fall vara fråga om information för att utreda hur en användare av mervärdestjänster rört sig eller information om användningen av en mervärdestjänst för att inrikta användningen av en metod för underrättelseinhämtning på en viss person.

Underrättelseinhämtning som avser datatrafik riktas mot datatrafik i kommunikationsnät som överskrider Finlands gräns, medan radiosignalspaning riktas mot radiovågor som sänds från eller till en anordning utanför finskt territorium. Underrättelseinhämtning som avser datatrafik riktas mot den del av kommunikationsnätet som specificeras i domstolens tillstånd och genom att använda de sökbegrepp som anges i tillståndet. Ett sökbegrepp som gäller meddelandets innehåll får användas endast när underrättelseinhämtning som avser datatrafik inriktas på en statlig aktör eller när det är fråga om information som beskriver innehållet i ett sabotageprogram. Med radiosignalspaning är det inte tillåtet att inhämta information om någon annans än en statlig aktörs meddelandeinnehåll. Indelningen av signalspaning i underrättelseinhämtning som avser datatrafik och radiosignalspaning är inte helt entydig

med tanke på avskiljandet av telekommunikation och radiokommunikation. Underrättelseinhämtning som avser utländska datasystem riktas mot datasystem utanför Finland. Gränsdragningen mellan underrättelseinhämtning som avser utländska datasystem och teknisk observation av utrustning kan lämna utrymme för tolkning.

Befogenheter avseende information

Från befogenheterna för informationsinhämtning som gäller en myndighets egna informationsinhämtningsåtgärder kan man avskilja myndighetens befogenheter avseende information, dvs. myndighetens rätt att få information, myndighetens rätt att behandla inhämtad information i sin egen verksamhet och myndighetens rätt att lämna ut information. Behandlingen av personuppgifter hos kriminalunderrättelsemyndigheter samt civila och militära underrättelsemyndigheter behandlas senare i samband med förhållandet mellan civil och militär underrättelseinhämtning och brottsbekämpning.

Regleringen av kriminalunderrättelsemyndigheters samt civila och militära underrättelsemyndigheters rätt att få information och rätt att lämna ut information bildar en komplex och strukturellt oenhetlig helhet. Det kan vara fråga om den utlämnande instansens rätt eller skyldighet att lämna ut information (och på motsvarande sätt den mottagande instansens möjlighet eller rätt att få information), utlämning av information som sker på eget initiativ eller på begäran samt utlämnande av enskilda uppgifter eller utlämnande av uppgifter genom en teknisk anslutning eller som en datamängd.

Den utlämnande instansens rätt att lämna ut annan information som gäller någon annan än instansen själv kan påverkas av dess lagstadgade eller avtalsbaserade sekretess- och tystnadsplikt. Utöver bestämmelser som uttryckligen gäller utlämnande av information kan rätten att lämna ut information också påverkas av bestämmelser om behandlingen av personuppgifter. Bestämmelserna om behandling av personuppgifter tillämpas på helt eller delvis automatiserad behandling av personuppgifter eller behandling av personuppgifter som sparas i register vid annan verksamhet än sådan som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll. Skyddet av personuppgifter handlar om en fysisk persons självbestämmanderätt avseende information. Personuppgifter är varje upplysning som direkt eller indirekt anknyter till en identifierad eller identifierbar fysisk person, dvs. även andra än sekretessbelagda eller känsliga uppgifter. Bland annat är utlämnande av personuppgifter behandling av personuppgifter. När det gäller elektronisk kommunikation omfattar dataskyddet förutom uppgifter som kan förenas till fysiska personer även uppgifter som kan förenas med juridiska personer.

Utlämnande av sekretessbelagda uppgifter eller personuppgifter kan basera sig på samtycke av den part vars intressen ska skyddas med sekretessplikten eller som omfattas av skyddet av personuppgifter, eller en lagstadgad rätt eller skyldighet att lämna uppgifterna eller en lagstadgad rätt att få uppgifterna. Samtycket till utlämnande av uppgifter kan gälla från fall till fall eller vara mer allmänt, till exempel givet i samband med godkännande av avtalsvillkor.

Skyddspolisen är en del av polisen. På dess rätt att få och lämna ut information tillämpas förutom kapitlet om civil underrättelseinhämtning i polislagen även de allmänna bestämmelserna i polislagen om polisens rätt att få information och polisens rätt

att lämna ut information trots av tystnadsplikten. Detta gäller skötseln av både kriminalunderrättelseuppdrag och civila underrättelseuppdrag. På Skyddspolisen tillämpas även specialbestämmelserna om Skyddspolisen i lagen om behandling av personuppgifter i polisens verksamhet samt lagens allmänna bestämmelser om polisens rätt att få uppgifter ur vissa register och polisens rätt att lämna ut personuppgifter. Rätten att få uppgifter ur vissa register omfattar även erhållande av uppgifter genom en teknisk anslutning eller som en datamängd.

Huvudstaben och Försvarsmaktens underrättelsetjänst är en del av Försvarsmakten. Om deras rätt att få information finns bestämmelser i fråga om kriminalunderrättelseverksamhet i lagen om militär disciplin och brottsbekämpning inom försvarsmakten och i fråga om militär underrättelseinhämtning i lagen om militär underrättelseverksamhet. På huvudstaben och Försvarsmaktens underrättelsetjänst tillämpas även bestämmelserna gällande Försvarsmaktens rätt att få personuppgifter för skötseln av militärunderrättelseuppdrag och uppdrag för förebyggande och avslöjande av brott i lagen om behandling av personuppgifter inom Försvarsmakten samt lagens allmänna bestämmelser om Försvarsmaktens rätt att lämna ut personuppgifter. Rätten att få uppgifter ur vissa register för skötseln av militärunderrättelseuppdrag och uppdrag för förebyggande och avslöjande av brott omfattar även erhållande av uppgifter genom en teknisk anslutning eller som en datamängd.

Med stöd av de allmänna bestämmelserna i polislagen om polisens rätt att få information och bestämmelserna om kriminalunderrättelseverksamhet i lagen om militär disciplin och brottsbekämpning inom försvarsmakten har kriminalunderrättelsemyndigheter och civila underrättelsemyndigheter rätt att för tjänsteuppdrag avgiftsfritt få behövlig information och handlingar av myndigheter och sammanslutningar som tillsatts för att sköta offentliga uppgifter, om inte överlämnande av informationen eller handlingarna till kriminalunderrättelsemyndigheten eller den civila underrättelsemyndigheten eller användning av informationen som bevis uttryckligen har förbjudits eller begränsats i lag. Uttrycken "överlämnande av informationen till den berörda myndigheten uttryckligen har förbjudits eller den har begränsats i lag" och "användning av informationen som bevis uttryckligen har förbjudits eller den har begränsats i lag" kan i praktiken vara flertydiga.

En privat sammanslutnings principiella skyldighet att hemlighålla sina kunders uppgifter som omfattas av företags-, bank- eller försäkringshemlighet eller andra uppgifter om kunderna kan basera sig på lag eller ett avtal som ingåtts med kunden. Enligt de allmänna bestämmelserna i polislagen om polisens rätt att få information har polisen trots företags-, bank- eller försäkringshemligheten rätt att av en privat sammanslutning få information som behövs för förebyggande eller utredning av brott. Rätten att få information anknyter till noggrant specificerade brott, men vilken information som ska fås har definierats på ett allmänt plan. Bestämmelser om civila och militära underrättelsemyndigheters rätt att få information av en privat sammanslutning trots företags-, bank- eller försäkringshemligheten finns i polislagens kapitel om civil underrättelseinhämtning och i lagen om militär underrättelseverksamhet. Rätten att få information anknyter till verksamhet som allvarligt hotar den nationella säkerheten, som definieras på ett allmänt plan, men informationen som ska fås är noggrannare specificerad. Det är fråga om information som kan antas vara av betydelse för att identifiera eller nå en person som är föremål för civil eller

militär underrättelseinhämtning eller för att utreda denna persons kontaktuppgifter eller rörelser, för att inrikta metoden för underrättelseinhämtning på en viss person som är föremål för civil eller militär underrättelseinhämtning eller för att utreda den ekonomiska verksamheten hos en person som är föremål för civil eller militär underrättelseinhämtning. I lagen om behandling av personuppgifter i polisens verksamhet och lagen om behandling av personuppgifter inom Försvarsmakten föreskrivs om kriminalunderrättelsemyndigheters samt civila och militära underrättelsemyndigheters rätt att få uppgifter om passagerare och resande av utövare av inkvarteringsverksamhet och trafikutövare.

Enligt de allmänna bestämmelserna om polisens rätt att få information i polislagen, bestämmelserna om kriminalunderrättelseverksamhet i lagen om militär disciplin och brottsbekämpning inom försvarsmakten samt bestämmelserna om militär underrättelseverksamhet i lagen om militär underrättelseverksamhet har kriminalunderrättelsemyndigheter samt civila och militära underrättelsemyndigheter rätt att av ett teleföretag och en sammanslutningsabonnent få kontaktuppgifter om en teleanslutning eller uppgifter som specificerar en teleanslutning eller teleterminalutrustning samt distributionsadressuppgifter av en sammanslutning som bedriver postverksamhet. Uppgifter som specificerar en teleanslutning eller teleterminalutrustning kan också inhämtas via myndighetens tekniska anordning (jfr inhämtande av basstationsuppgifter med teleföretagets hjälp).

Ett tillstånd som domstolen beviljat kriminalunderrättelsemyndigheter eller civila eller militära underrättelsemyndigheter för inhämtande av information genom teleavlyssning, inhämtande av information i stället för teleavlyssning eller teleövervakning skapar en lagstadgad skyldighet för teleföretagen och en lagstadgad rätt för sammanslutningsabonnenter att utlämna den information som tillståndet omfattar till myndigheten.

Behandlingen av uppgifter i samband med sabotageprogram utgör ett specialfall. I detta fall kan det vara frågan om till exempel möjligheten för en innehavare av informationssystem eller en kommunikationsförmedlare eller en leverantör av en mervärdestjänst att förutom uppgifter om sig själv även lämna ut information som kan förenas med informationssystemets, kommunikationstjänstens eller mervärdestjänstens användare utan användarnas samtycke, om utlämnandet av information är nödvändigt för att tillgodose informationssäkerheten i informationssystemet, kommunikationstjänsten eller mervärdestjänsten. Tillgodoseendet av den personuppgiftsansvariges berättigade intressen och iakttagandet av den personuppgiftsansvariges lagstadgade skyldighet kan utgöra en grund för lagenligheten i dess behandling av personuppgifter. I lagen om tjänster inom elektronisk kommunikation åläggs kommunikationsförmedlare och leverantörer av mervärdestjänster att sörja för informationssäkerheten. I lagen föreskrivs också om skyldigheten för kommunikationsförmedlare och leverantörer av mervärdestjänster att underrätta meddelandets avsändare och mottagare om manuell behandling av meddelandets innehåll i samband med informationssäkerhetsåtgärder, om det inte är så att underrättelsen sannolikt äventyrar informationssäkerheten. I lagen finns även bestämmelser om meddelandet till tjänstens användare om teleföretagets tjänster eller mervärdestjänster, marknadsplatser, sökmotortjänster och molntjänster har utsatts för kräkningar av informationssäkerheten. Det föreskrivs särskilt om den personuppgiftsansvariges skyldighet att informera den registrerade om en personuppgiftsincident.

Inriktning av informationsinhämtning

Vid kriminalunderrättelseverksamhet inriktas informationsinhämtningen på en person som antas göra sig skyldig eller misstänks ha gjort sig skyldig till ett brott. Personen kan också vara okänd i början av informationsinhämtningen.

Vid civil och militär underrättelseinhämtning är föremålet för informationsinhämtningen verksamheten hos en aktör som orsakar ett hot mot den nationella säkerheten. Informationsinhämtningen inriktas i allmänhet på en person som orsakar ett hot. Det kan till exempel vara frågan om en representant för en främmande stat eller en medlem i en terroristgrupp eller organiserad kriminell grupp.

På grund av syftet med och föremålen för civil och militär underrättelseinhämtning kan civil och militär underrättelseinhämtning riktas även mot sådan organisationsverksamhet av en främmande stat eller annan aktör som hotar den nationella säkerheten, som inte har en fast koppling till en viss, specificerad person eller specificerade personer (jfr tillräckligt specificerad grupp av personer). Det kan till exempel röra sig om en främmande stats militära verksamhet. Även bakom organisationsverksamhet finns enskilda personer, som dock kan vara oidentifierade för närvarande eller mer permanent. När det gäller användningen av underrättelseinhämtningsmetoder ska förutsättningarna för användningen av metoderna uppfyllas också när de enskilda personer som ligger bakom organisationsverksamheten är oidentifierade.

Bland annat har riksdagens justitieombudsman lyft fram frågan om subjektiv inriktande av användningen av metoder för underrättelseinhämtning vid civil och militär underrättelseinhämtning. Då grunden för definieringen av metoder för underrättelseinhämtning vid civil underrättelseinhämtning är regleringen i kapitlet om hemliga metoder för inhämtande av information i polislagen, föreskrivs det inte närmare i fråga om underrättelseinhämtningsmetoderna om vilka personer informationsinhämtningen kan riktas på. I detta fall begränsas inriktningen av informationsinhämtningen snarast av de allmänna förutsättningarna för användningen av metoderna för underrättelseinhämtning och principerna för civil underrättelseinhämtning. När det gäller militär underrättelseverksamhet föreskrivs det att informationsinhämtningen kan inriktas på en person med anknytning till ett underrättelseuppdrag. En person med anknytning till ett underrättelseuppdrag kan förutom den egentliga orsakaren av hotet också vara en person som anknyter till den egentliga orsakaren av hotet. Det antas då att inriktningen av informationsinhämtningen på denna person har en mycket stor betydelse när det gäller att få sådan information som berör den verksamheten hos den egentliga orsakaren av hotet. Personens anknytning till den egentliga orsakaren av hotet kan beroende på omständigheterna framgå till exempel som kontakter mellan personen och den egentliga orsakaren av hotet.

En person som är föremål för verksamhet som hotar den nationella säkerheten torde inte i allmänhet kunna betraktas som en person med en ovan avsedd anknytning till ett underrättelseuppdrag. Ett slags undantag till detta torde dock kunna utgöras av situationer som behandlas nedan i samband med inriktning av åtgärder för inhämtande av information och bekämpning av sabotageprogram, där en aktör som utgör ett hot mot den nationella säkerheten använder en persons utrymme eller en plats av annat slag,

föremål, ämne eller egendom, teknisk anordning eller dess programvara eller teleadress eller teleterminalutrustning i hemlighet eller genom vilseledning.

Öppen informationsinhämtning i anslutning till förundersökning av brott, bland annat förhör och en del av andra än hemliga tvångsmedel får inriktas även på personer som är föremål för kriminell verksamhet (målsägande i brott) också utan dennes samtycke.

Inriktning av åtgärder för informationsinhämtning

I kriminalunderrättelseverksamhet inriktas användningen av befogenheten för informationsinhämtning vid systematisk observation, förtäckt inhämtande av information och täckoperation på en person, vid teknisk avlyssning och optisk observation på ett utrymme eller en plats av annat slag, vid teknisk spårning på ett föremål, ämne eller egendom, vid teknisk observation av utrustning på en teknisk anordning eller dess programvara samt vid teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning på en teleadress eller teleterminalutrustning. Det föreskrivs särskilt om teknisk spårning av en person, dvs. att följa hur en person förflyttar sig genom att en spårningsanordning fästs i de kläder som personen bär eller i ett föremål som personen bär med sig. När kriminalunderrättelseverksamhet inriktas på en person som antas göra sig skyldig eller misstänks ha gjort sig skyldig till ett brott, ska vid kriminalunderrättelseverksamhet även utrymmet eller platsen av annat slag, föremålet, ämnet eller egendomen, den tekniska anordningen eller dess programvara eller teleadressen eller teleterminalutrustningen som är föremål för åtgärden för informationsinhämtning anknyta till den berörda personen. Det är fråga om ett utrymme eller plats av annat slag, där den person som är föremål för informationsinhämtning vistas eller besöker med tillstånd, eller ett föremål, ämne eller egendom, en teknisk anordning eller dess programvara eller en teleadress eller teleterminalutrustning som personen som är föremål för inhämtandet av information innehar eller som personen i övrigt använder med tillstånd. Teknisk spårning kan också riktas på ett föremål, ämne eller egendom som är föremål för ett brott.

I kriminalunderrättelseverksamhet utgörs ett undantag till kravet på att metoden för inhämtande av information ska anknyta till den person som är det egentliga föremålet för informationsinhämtningen av teleövervakning med samtycke av teleadressens eller teleterminalutrustningens innehavare och av inhämtande av basstationsuppgifter. Vid teleövervakning med samtycke av teleadressens eller teleterminalutrustningens innehavare kan samtycke ges av den brottsmisstänkte, målsäganden, ett vittne eller någon annan person. Grunden för teleövervakning som baserar sig på samtycke av teleadressens eller teleterminalutrustningens innehavare kan vara bland annat ett brott på grund av vilket teleadressen eller teleterminalutrustningen olovligen är i någon annans besittning (identifieringsuppgifter för meddelanden som sänts från målsägandens teleadress eller teleterminalutrustning), och ett brott som begåtts med hjälp av teleadressen eller teleterminalutrustningen (identifieringsuppgifter för meddelanden som mottagits till målsägandens teleadress eller teleterminalutrustning). Vid inhämtande av basstationsuppgifter inhämtas information om alla teleterminalutrustningar eller teleadresser som loggat in eller loggar in till telesystemet via en viss basstation.

I civil och militär underrättelseinhämtning får användningen av befogenheten för informationsinhämtning inte riktas på ett utrymme som används för boende av permanent natur. Fritidsbostäder kan åtnjuta ett sådant hemfridsskydd för utrymmen som används för boende av permanent natur, trots att man inte bor i dem året runt. Även när det gäller kriminalunderrättelseverksamhet är det i regel förbjudet att rikta befogenheten för inhämtande av information mot ett utrymme som används för boende av permanent natur. I kriminalunderrättelseverksamhet är täckoperationer och bevisprovokation genom köp i en bostad dock tillåtna, om tillträdet eller vistelsen sker med aktiv medverkan av den som använder bostaden. Vid kriminalunderrättelseverksamhet som stöder utredning av brott är det möjligt att rikta teknisk avlyssning även mot utrymmen som används för boende av permanent natur.

Vid civil och militär underrättelseinhämtning kan systematisk observation, förtäckt inhämtande av information och täckoperationer inriktas på personer, men också på grupper av personer. Teknisk avlyssning och optisk observation kan inriktas på ett utrymme eller plats av annat slag samt på en person eller en grupp av personer. Teknisk spårning kan inriktas på ett föremål, ett ämne eller en egendom samt på en person. Teleavlyssning, inhämtande av information i stället för teleavlyssning och teleövervakning kan inriktas på en teleadress eller teleterminalutrustning, men också på en person.

Då civil och militär underrättelseinhämtning kan inriktas också mot sådan organisationsverksamhet som hotar den nationella säkerheten och som inte har en fast koppling till en viss, specificerad person eller vissa specificerade personer, är det i civil och militär underrättelseinhämtning också möjligt att inrikta åtgärden för inhämtande av information på ett utrymme eller en plats av annat slag, ett föremål, ämne eller egendom, en teknisk anordning eller dess programvara eller en teleadress eller teleterminalutrustning som används i organisationsverksamhet som hotar den nationella säkerheten utan en uttrycklig koppling till en person. Det kan till exempel vara frågan om ett utrymme eller en plats av annat slag, ett föremål, ämne eller egendom, en teknisk anordning eller dess programvara eller en teleadress eller teleterminalutrustning som en främmande stat använder i sin militära verksamhet. Teleadresser och teleterminalutrustning som används för att sända och ta emot förtroliga meddelanden har emellertid i allmänhet även i detta fall en koppling till en viss person eller vissa personer. Detta stöder säkerställandet av att åtgärden för inhämtande av information inriktas på verksamheten hos den aktör som är föremål för informationsinhämtningen, dvs. att man vid inhämtandet av information ingriper i hemligheten i ett förtroligt meddelande så riktat och begränsat som möjligt (se även avbrytande av teleavlyssning som behandlas nedan i samband med de allmänna förutsättningarna för användning av underrättelseinhämtningsmetoder samt principerna för civil och militär underrättelseinhämtning). Om föremålet för informationsinhämtningsåtgärden inte har en fast koppling till en viss specificerad person eller vissa specificerade personer, kan risken för att informationsinhämtningen i själva verket riktas mot utomstående vara större än vanligt.

Teleövervakning med samtycke av teleadressens eller teleterminalutrustningens innehavare och inhämtande av basstationsuppgifter utgör även i civil och militär underrättelseinhämtning ett undantag till kravet på koppling till den aktör som är det egentliga föremålet för informationsinhämt-

ning hos föremålet för åtgärden för inhämtande av information. Till skillnad från elementär teleövervakning som kräver ett domstolstillstånd, beslutar underrättelsemyndigheten i civil och militär underrättelseinhämtning själv om teleövervakning med samtycke av teleadressens eller teleterminalutrustningens innehavare. I kriminalunderrättelseverksamhet omfattar underrättelsemyndighetens rätt att själv besluta om teleövervakning med samtycke av teleadressens eller teleterminalutrustningens innehavare endast en del av grunderna för teleövervakning, medan domstolen beslutar om teleövervakning med samtycke av teleadressens eller teleterminalutrustningens innehavare när det gäller andra grunder.

Information om kriminell verksamhet eller verksamhet som hotar den nationella säkerheten som är föremål för kriminalunderrättelseverksamhet eller civil och militär underrättelseinhämtning kan också fås med hjälp av informationsinhämtning som inriktas på ett utrymme eller en plats av annat slag, föremål, ämne eller egendom, teknisk anordning eller dess programvara eller teleadress eller teleterminalutrustning som är föremål för verksamheten. En person som är föremål för kriminell verksamhet eller verksamhet som hotar den nationella säkerheten kan ge kriminalunderrättelsemyndigheten eller den civila eller militära underrättelsemyndigheten frivilligt information som gäller honom eller henne själv och ett utrymme eller en plats av annat slag, föremål, ämne eller egendom, teknisk anordning eller dess programvara eller teleadress eller teleterminalutrustning som tillhör honom eller henne samt ovan avsedda samtycke till teleövervakning av teleadress eller teleterminalutrustning. I en situation där en aktör som orsakar ett hot mot den nationella säkerheten använder personens utrymme eller plats av annat slag, föremål, ämne eller egendom, teknisk anordning eller dess programvara eller teleadress eller teleterminalutrustning i verksamhet som hotar den nationella säkerheten i hemlighet eller genom att vilseleda personen, kan det uppstå ett behov av att inrikta inhämtande av information mot utrymmet eller platsen av annat slag, föremålet, ämnet eller egendomen, den tekniska anordningen eller dess programvara eller teleadressen eller teleterminalutrustningen även utan personens samtycke och även i hemlighet för honom eller henne. Behovet kan uppstå till exempel i samband med bekämpning av sabotageprogram, som behandlas härnäst.

Bekämpning av sabotageprogram

Sabotageprogram kan vara till exempel virus som förstör eller förändrar data, spionprogram som samlar data eller program som gör en teknisk anordning och dess programvara till en del av ett så kallat botnätverk. När ett skadligt datorprogram installeras på en teknisk anordning eller när den tekniska anordningens programvara ges ett skadligt kommando, tas den tekniska anordningen och dess programvara i bruk olovligt. Att förstöra eller förändra data kan uppfylla rekvisitet för dataskadegörelse eller systemstörning och att samla in data kan uppfylla rekvisitet för dataintrång. En teknisk anordning och dess programvara som tagits med som en del av ett botnätverk används som redskap för vidaresändning av sabotageprogram. Skadliga datorprogram och kommandon är hjälpmedel vid nätbrott, där bara behandlingen kan uppfylla rekvisitet för orsakande av fara för informationsbehandling eller innehav av hjälpmedel vid nätbrott.

Vid en kränkning av informationssäkerheten i anslutning till elektronisk kommunikation skickas meddelandets mottagare ett meddelande som innehåller ett skadligt datorprogram eller kommando. Vid sändning av ett meddelande som innehåller ett skadligt datorprogram eller kommando till mottagaren i skadligt syfte är det inte fråga om konfidentiell kommunikation mellan avsändaren och mottagaren. Meddelanden som orsakas av spionprogrammens funktion är ett kapitel för sig. Inte heller i dessa är det fråga om konfidentiell kommunikation mellan avsändaren och mottagaren, och meddelanden orsakade av spionprogrammets funktion kan dessutom ha en indirekt inverkan på förtroligheten i elektronisk kommunikation hos de aktörer som är föremål för spionprogrammet och samtidigt helt utomstående aktörer.

Föremålet för civil underrättelseinhämtning kan vara verksamhet som hotar samhällets vitala funktioner. Föremålet för militär underrättelseinhämtning kan vara en främmande stats verksamhet eller någon annan verksamhet som äventyrar samhällets vitala funktioner. Samhällets vitala funktioner kan äventyras av bland annat kränkningar av informationssäkerheten som inriktas på informationssystem och datatrafikarrangemang som anknyter till samhällets vitala funktioner. Det kan röra sig om informationssystem och datatrafikarrangemang som används av både myndigheter och privata aktörer. Det är snarast främmande stater och andra organisationsaktörer som kan ha förmågan att orsaka ett allvarligt hot mot informationssystem och datatrafikarrangemang som anknyter till samhällets vitala funktioner. Genom informationsinhämtning som gäller kränkningar av informationssäkerheten orsakade av sådana aktörer kan man stöda informationssäkerhetsåtgärderna hos innehavare av informationssystem och kommunikationsförmedlare samt sammanställa en lägesbild och skapa ett informationsunderlag för den högsta statsledningens beslutsfattande och säkerhetsmyndigheternas påverkansåtgärder, inklusive användning av cybermaktmedel. Om användningen av maktmedel föreskrivs i kapitlet om polisens allmänna befogenheter i polislagen, territorialövervakningslagen och lagen om försvarsmakten.

Frågan gällande rätten för innehavare av informationssystem eller kommunikationsförmedlare eller leverantörer av mervärdestjänster att lämna ut information för att sörja för informationssystemets eller kommunikationstjänstens eller mervärdestjänstens informationssäkerhet behandlas ovan i samband med befogenheterna avseende information.

I civil och militär underrättelseinhämtning kan informationsinhämtning som gäller kränkningar av informationssäkerheten i informationssystem och datatrafikarrangemang som anknyter till samhällets vitala funktioner utgöra ett undantag när det gäller inriktning av informationsinhämtning och åtgärder för inhämtande av information. Vid bekämpningen av sabotageprogram kan det behövas information som anger hur meddelandet som innehåller sabotageprogrammet förmedlas i kommunikationsnät och/eller beskriver meddelandets innehåll och det skadlig programmets funktion. I civil och militär underrättelseinhämtning torde en person som anknyter till ett underrättelseuppdrag kunna anses vara innehavaren av en sådan teknisk anordning, vars tekniska anordning har tagits i bruk olovligen genom att placera ett skadligt datorprogram i anordningen eller genom att ge dess programvara ett skadligt kommando. I civil och militär underrättelseinhämtning torde man av denna anledning kunna rikta teleavlyssning,

inhämtande av information i stället för teleavlyssning och elementär teleövervakning mot den teleadress eller teleterminalutrustning som är föremål för meddelandet som innehåller sabotageprogrammet samt teknisk observation av utrustning mot den tekniska anordning som är föremål för sabotageprogrammet inom de ramar som de nedan angivna allmänna förutsättningarna för metoder för underrättelseinhämtning samt principerna för civil och militär underrättelseinhämtning tillåter till den del som informationsinhämtningen inte kan riktas direkt på den aktör som utgör ett allvarligt hot mot informationssystem och datatrafikarrangemang som anknyter till samhällets vitala funktioner. Det kan vara nödvändigt att genomföra sådan informationsinhämtning utan att avslöja det för innehavaren av teleadressen eller teleterminalutrustningen som är föremål för ett meddelande som innehåller ett sabotageprogram eller innehavaren av en teknisk anordning som är föremål för ett sabotageprogram av de anledningar som behandlads nedan i samband med skydd och sekretess vid inhämtande av information.

Inga uttryckliga uppgifter eller befogenheter har föreskrivits för civila och militära underrättelsemyndigheter i Finland när det gäller stödjande av informationssäkerheten i informationssystem och datatrafikarrangemang i anslutning till samhällets vitala funktioner. Till exempel i de övriga nordiska länderna är situationen delvis en annan.

Också i Finland har Skyddspolisen till uppgift att ge myndigheter och sammanslutningar sådana anvisningar, råd och uppgifter som behövs för att upprätthålla den nationella säkerheten eller för att förhindra kränkningar av den. Enligt lagen om behandling av personuppgifter i polisens verksamhet får Skyddspolisen, för att sköta sina uppgifter, trots sekretessbestämmelserna lämna ut personuppgifter till andra myndigheter eller till sammanslutningar som sköter offentliga uppgifter samt trots sekretessbestämmelserna i enskilda fall lämna ut personuppgifter till privata sammanslutningar och personer, om det finns vägande skäl och om det är nödvändigt för att Skyddspolisen ska kunna utföra sina uppgifter. Enligt de allmänna bestämmelserna i polislagen om utlämnande av uppgifter trots bestämmelserna om tystnadsplikt förhindrar tystnadsplikten för en person som hör till polisens personal inte röjande av sådana uppgifter för vars röjande det i enskilda fall finns ett vägande skäl för förhindrande av en händelse som äventyrar liv eller hälsa eller ett brott som riktar sig mot friheten eller betydande skada på miljön eller betydande egendoms- eller förmögenhetsskada eller för tryggande av den nationella säkerheten. Enligt kapitlet om civil underrättelseinhämtning i polislagen får Skyddspolisen för att genomföra sitt uppdrag avseende civil underrättelseinhämtning trots sekretessbestämmelserna lämna ut andra uppgifter än personuppgifter till andra myndigheter, företag och andra sammanslutningar, om utlämnandet av uppgifterna i fråga om andra myndigheter behövs samt i fråga om företag och andra sammanslutningar är nödvändigt för att skydda den nationella säkerheten.

Enligt bestämmelserna om utlämnande av personuppgifter i lagen om behandling av personuppgifter inom Försvarsmakten får Försvarsmakten trots sekretessbestämmelserna lämna ut personuppgifter som behövs till en annan myndighet, en sammanslutning och en privatperson för att avvärja en betydande fara för någons liv, hälsa eller frihet eller en ansenlig miljö-, egendoms- eller förmögenhetsskada. Enligt lagen om militär underrättelseverksamhet får militärunderrättel-

semyndigheterna för att genomföra sitt uppdrag, trots sekretessbestämmelserna lämna ut andra uppgifter än personuppgifter till andra myndigheter, om utlämnandet av uppgifterna är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten, och andra uppgifter än personuppgifter till företag och andra sammanslutningar, om utlämnandet av uppgifterna är nödvändigt med avseende på Försvarsmaktens verksamhet eller för att skydda den nationella säkerheten.

De så kallade brandväggsbestämmelserna, som behandlas nedan i samband med förhållandet mellan civil och militär underrättelseinhämtning och brottsbekämpning, möjliggör att information som inhämtats med hjälp av en metod för underrättelseinhämtning lämnas ut bland annat för att avvärja en betydande fara för någons liv, hälsa eller frihet eller en ansenlig miljö-, egendoms- eller förmögenhetsskada.

I lagen om militär underrättelseverksamhet föreskrivs särskilt att militärunderrättelsemyndigheterna trots sekretessbestämmelserna till företag och andra sammanslutningar kan lämna ut identifieringsuppgifter som anknyter till sabotageprogram och som behövs för utvecklingen av metoder och system för underrättelseinhämtning, om utlämnandet av uppgifterna är nödvändigt med avseende på Försvarsmaktens verksamhet eller för att skydda den nationella säkerheten. I lagen om civil underrättelseinhämtning avseende datatrafik och i lagen om militär underrättelseverksamhet föreskrivs särskilt att civila och militära underrättelsemyndigheter trots sekretessbestämmelserna får lämna ut sådan information som inhämtats med hjälp av underrättelseinhämtning som avser datatrafik och som gäller skadliga datorprogram eller skadliga datakommandon och deras verkningar till myndigheter, företag eller sammanslutningar, om utlämnandet av informationen behövs för att skydda den nationella säkerheten eller informationsmottagarens intressen.

Allmänna förutsättningar för användning av metoder för underrättelseinhämtning samt principer för civil och militär underrättelseinhämtning

Föremålen för informationsinhämtning, inriktning av informationsinhämtning och inriktning av åtgärder för inhämtande av information, vilka behandlas ovan, är inte lika strikt reglerade i och militär underrättelseinhämtning som i kriminalunderrättelseverksamhet och civil och militär underrättelseinhämtning omfattas av ett större skydd och sekretess än kriminalunderrättelseverksamhet. Vid prövningen av användningen av en metod för underrättelseinhämtning betonas därför betydelsen av bedömningen av allvarsgraden i hotet mot den nationella säkerheten samt av de allmänna förutsättningarna för användningen av metoder för underrättelseinhämtning och av principerna för civil och militär underrättelseinhämtning. Enligt de allmänna förutsättningarna för användning av metoder för underrättelseinhämtning ska användningen av metoden för underrättelseinhämtning kunna antas ge viktig information med tanke på underrättelseuppdraget. Enligt proportionalitetsprincipen ska underrättelseinhämtningens åtgärder vara försvarbara i förhållande till hur viktiga de uppgifter är som erhålls genom informationsinhämtningen, till hur brådskande underrättelseuppdraget är, till det eftersträvade målet för underrättelseinhämtningen, till föremålet för underrättelseinhämtningen och till den inskränkning av rättigheter som andra orsakas av att en underrättelseåtgärd används.

De allmänna förutsättningarna för användningen av metoder för underrättelseinhämtning samt principerna för civil och militär underrättelseinhämtning ska beaktas även när behovet av att inkludera begränsningar eller villkor i domstolens eller civil- eller militärunderrättelsemyndighetens beslut om användning av metoden för underrättelseinhämtning prövas. Enligt principen om minsta olägenhet får det inte ingripas i någons rättigheter i större utsträckning och ingen får orsakas större skada eller olägenhet än vad som är nödvändigt för att utföra uppdraget. Vid underrättelseinhämtning ska ingrepp i skyddet för hemligheten i fråga om förtroliga meddelanden ske så riktat och begränsat som möjligt.

Betydelsen av bedömningen av huruvida förutsättningarna för användning av en metod för underrättelseinhämtning uppfylls samt de begränsningar och villkor som vid behov inkluderas i beslutet om användningen av metoden för underrättelseinhämtning understryks i situationer där informationsinhämtning gällande verksamheten hos en aktör som orsakar ett hot mot den nationella säkerheten riktas de facto mot en aktör som är föremål för verksamhet som hotar den nationella säkerheten eller en helt utomstående aktör. Till exempel är det möjligt att genom informationsinhämtning som gäller elektronisk kommunikation också få information om kommunikation som inte anknyter till verksamhet som hotar den nationella säkerheten mellan den person som är föremål för informationsinhämtning och utomstående. Informationsinhämtning som anknyter till bekämpning av sabotageprogram torde kunna genomföras också på det sätt som anges ovan, där åtgärden för informationsinhämtning riktas mot den teleadress eller teleterminalutrustning är föremål för ett meddelande som innehåller sabotageprogrammet eller den tekniska anordning som är föremål för sabotageprogrammet.

Bredden och djupet i ingreppet i hemligheten i ett förtroligt meddelande och i det övriga skyddet av privatlivet i anslutning till bekämpning av sabotageprogram kan påverkas av huruvida man genom informationsinhämtningen endast utreder hur meddelandet som innehåller ett sabotageprogram förmedlas i kommunikationsnätet eller sabotageprogrammets tekniska funktion eller också kartlägger data och information som spionprogrammet insamlar. Om informationsinhämtningen som riktas mot en teleadress eller teleterminalutrustning som är föremål för ett meddelande som innehåller ett sabotageprogram eller en teknisk anordning som är föremål för ett sabotageprogram gäller innehållen i meddelanden som orsakas av spionprogrammets funktion, kan det i samband med informationsinhämtningen förutom data som spionprogrammet insamlat rörande den nationella säkerheten också avslöjas uppgifter som spionprogrammet insamlat om en helt utomstående aktör.

Det kan vara möjligt att tekniskt rikta och begränsa ingreppet i hemligheten i fråga om förtroliga meddelanden och i det övriga skyddet av privatlivet genom att filtrera nödvändig information med tanke på underrättelseuppdraget ur kommunikationen som är föremål för informationsinhämtningen med hjälp av automatisk behandling (jfr bestämmelserna om informationssäkerhetsåtgärder för kommunikationsförmedlare och leverantörer av mervärdestjänster i lagen om tjänster inom elektronisk kommunikation samt lagens specialreglering gällande sammanslutningsabonnenter). Det kan till exempel vara fråga om att man ur kommunikationen kan välja meddelanden som innehåller sabotageprogram på basis av meddelandets typ, form eller andra motsvarande egenskaper och/eller att det är möjligt att lösgöra information som beskriver sabotageprogrammets

tekniska funktion ur innehållet i meddelandena. Om behövliga uppgifter med tanke på underrättelseuppdraget inte kan filtreras på det sätt som avses ovan, ska den information som behövs för underrättelseuppdraget eller för att i övrigt skydda den nationella säkerheten avskiljas från annan information manuellt i samband med granskningen av det material som erhållits genom användning av underrättelseinhämtningsmetoden.

Regleringen av civil och militär underrättelseinhämtning, som inte är lika strikt som regleringen av kriminalunderrättelseverksamhet, samt skyddet och sekretessen, som är mer omfattande i civil och militär underrättelseinhämtning än i kriminalunderrättelseverksamhet, ska balanseras även i andra situationer genom noggrann granskning av det material som erhållits genom användning av underrättelseinhämtningsmetoder och effektiv övervakning av denna granskning. Vid granskningen av materialet som erhållits genom att använda metoder för underrättelseinhämtning ska det säkerställas att materialet gäller verksamhet hos den aktör som är föremål för informationsinhämtning. En person som är föremål för informationsinhämtning kan vara tills vidare oidentifierad och en representant för en organisation som är föremål för informationsinhämtning kan vara mer permanent oidentifierad. Till granskningen av materialet som erhållits genom att använda metoder för underrättelseinhämtning anknyter vid behov avbrytande av användningen av metoden för underrättelseinhämtning och utplåning av materialet som erhållits genom användning av metoden för underrättelseinhämtning.

När det gäller kriminalunderrättelseverksamhet och militär underrättelseverksamhet föreskrivs det om avbrytande av teleavlyssning, teknisk avlyssning och teknisk observation av utrustning samt utplåning av tillhörande upptagningar och anteckningar, om det framgår att teleavlyssningen riktas mot något annat meddelande än ett meddelande från eller till den som är föremål för tillståndet eller att den person som den tekniska avlyssningen riktas mot inte befinner sig i det utrymme eller på den plats av annat slag som avlyssnas eller om det framgår att den person som är föremål för teknisk observation av utrustning inte använder den anordning som är föremål för observationen. Det finns inga motsvarande bestämmelser om avbrytande av optisk observation. När det gäller civil underrättelseinhämtning finns inga bestämmelser om avbrytande av användningen av befogenheter för informationsinhämtning.

I fråga om kriminalunderrättelseverksamhet föreskrivs det om utplåning av information som erhållits genom teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter och teknisk observation (teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning). När det gäller kriminalunderrättelseverksamhet som stöder förebyggande av brott och avslöjande av brott är det fråga om information som inte behövs för förebyggande, avslöjande eller utredning av brott eller för avvärjande av fara. I fråga om kriminalunderrättelseverksamhet som stöder utredning av brott handlar det om information som inte har samband med brottet eller som gäller ett annat brott än det för vars utredning tillståndet eller beslutet har getts, efter det att det ursprungliga ärendet har avgjorts med laga kraft eller lämnats utan prövning. När det gäller civil underrättelseinhämtning föreskrivs det om utplåning av sådan information som fås genom en metod för underrättelseinhämtning som inte behövs för att skydda den nationella säkerheten, och i fråga om militär underrättelseinhämtning om utplåning av sådan information som fås genom

en metod för underrättelseinhämtning som inte behövs eller får användas för att sköta uppgifter inom militär underrättelseinhämtning eller som inte är behövligt med avseende på försvaret av landet eller för att skydda den nationella säkerheten. Information som i övrigt föreskrivits att ska utplånas kan dock bevaras och lagras i register i kriminalunderrättelseverksamhet i de fall som avses i bestämmelserna om användningen av överskottsinformation samt i civil och militär underrättelseinhämtning i de fall som avses i de så kallade brandväggsbestämmelserna, vilka behandlas nedan i samband med förhållandet mellan civil och militär underrättelseinhämtning och brottsbekämpning.

Skydd och sekretess vid inhämtande av information

Behovet av att skydda och hemlighålla kriminalunderrättelseverksamhet samt civil och militär underrättelseinhämtning eller detaljer rörande dem från allmänheten, en aktör som är föremål för informationsinhämtning och eventuellt även från en aktör som är föremål för kriminell verksamhet eller verksamhet som hotar den nationella säkerheten kan bero på tryggandet av en pågående informationsinhämtningsoperation samt i fråga om långsiktig informationsinhämtning avseende professionell och fortgående organisationsverksamhet även tryggandet av kommande informationsinhämtningsoperationer. I synnerhet i samband med informationsinhämtning som gäller professionell verksamhet understryks också behovet av att hemlighålla kriminalunderrättelsemyndigheters samt civila och militära underrättelsemyndigheters taktiska och tekniska metoder och planer. En förutsättning för kontinuiteten för utbyte av konfidentiell information i anslutning till verksamhet med informationskällor och internationellt samarbete är att verksamheten förblir konfidentiell. Behovet av sekretess i informationsinhämtning kan också hänföra sig till skyddandet av underrättelsetjänstemännens och informationskällornas säkerhet.

Möjligheten att skydda civil och militär underrättelseinhämtning har definierats som mer omfattande än skyddet av kriminalunderrättelseverksamhet. I fråga om civil och militär underrättelseinhämtning handlar det om åtgärder som är nödvändiga för att skydda den civila och militära underrättelseinhämtningen. När det gäller kriminalunderrättelseverksamhet är det fråga om åtgärder som är nödvändiga för att skydda användningen av en hemlig metod för informationsinhämtning eller ett hemligt tvångsmedel som pågår, redan har genomförts eller ska genomföras i framtiden. I en informationsinhämtningsoperation kan flera befogenheter för informationsinhämtning användas samtidigt eller efter varandra.

Enligt offentlighetslagen blir information om brott som redan begåtts i regel offentliga för allmänheten, då ärendet har behandlats i ett domstolssammanträde, åklagaren har beslutat att inte väcka åtal i ärendet eller ärendet har lämnats utan prövning. Utredningar som gäller förebyggande av brott är sekretessbelagda under en längre tid. Den allmänna offentligheten för civil och militär underrättelseinhämtning är begränsad i ännu större omfattning och mer långvarigt.

Det särskilda sekretessintresse som förknippas med ärenden som rör den nationella säkerheten återspeglas också i straffbestämmelserna om obehörigt röjande av informationen. Obehörigt röjande av en upplysning som ska hemlighållas på grund av den nationella säkerheten straffas som röjande av statshemlighet, medan obehörigt

röjande av en annan sekretessbelagd upplysning straffas som brott mot tjänstehemlighet i fråga om tjänstemän, personer som utövar offentlig makt och offentligt anställda arbetstagare samt i fråga om andra personer som sekretessbrott.

Hemliga metoder för informationsinhämtning och hemliga tvångsmedel i kriminalunderrättelseverksamhet och underrättelseinhämtningsmetoder i civil och militär underrättelseinhämtning kan användas och används också i allmänhet i hemlighet för den som är föremål för informationsinhämtningen. Den person som är föremål för informationsinhämtning ska underrättas om användningen av vissa befogenheter för inhämtande av information efter det att målet med användningen av befogenheten har uppnåtts. En domstol kan på de i lagen föreskrivna grunderna besluta att underrättelsen får skjutas upp eller lämnas ogjord. Föremålet för informationsinhämtning ska underrättas om användningen av vissa befogenheter för informationsinhämtning, om förundersökning har inletts i ärendet och ärendet har lämnats till åklagaren för prövning. I civil och militär underrättelseinhämtning föreligger ingen skyldighet att underrätta föremålet för informationsinhämtningen om föremålet i användningen av metoden för underrättelseinhämtning har varit en statlig aktör eller därmed jämförbar aktör.

När hemlig informationsinhämtning avseende verksamheten hos en aktör som utgör ett hot mot den nationella säkerheten i civil och militär underrättelseinhämtning riktas de facto också mot en aktör som är föremål för verksamhet som hotar den nationella säkerheten till exempel på det sätt som behandlas ovan i samband med bekämpning av sabotageprogram, är det motiverat att särskilt bedöma om en sådan aktör som är föremål för verksamhet som hotar den nationella säkerheten ska informeras om användningen av metoden för underrättelseinhämtning och det hot som den grundar sig på, trots att man skulle låta bli att informera den aktör som har orsakat hotet för den nationella säkerheten och varit det egentliga föremålet för användning av metoden för underrättelseinhämtning direkt med stöd av lag (statlig aktör eller därmed jämförbar aktör) eller med stöd av ett domstolsbeslut (annan aktör). Vid bedömningen ska intresset för skyddande av den nationella säkerheten och tillhörande skydds- och sekretessbehov vid civil och militär underrättelseinhämtning vägas upp mot sådana allmänna och enskilda intressen, såsom förhindrande eller begränsning av konkreta skador och olägenheter som orsakas av verksamhet som hotar den nationella säkerheten.

Att användningen av befogenheter för informationsinhämtning blir partsoffentliga är både i fråga om kriminalunderrättelseverksamhet och civil och militär underrättelseinhämtning kopplad till underrättande av den person som varit föremål för informationsinhämtning om användningen av befogenheten för informationsinhämtning. Förhållandet mellan bestämmelser om begränsning av partsoffentlighet i speciallagar och de allmänna bestämmelserna om partsoffentlighet i offentlighetslagen förblir dock delvis flertydig när det gäller bestämmelsernas tillämpningssituationer, specificering av part och grunderna för begränsning av partsoffentligheten. Till skillnad från kriminalunderrättelseverksamhet föreskrivs det inte särskilt för civil och militär underrättelseinhämtning om möjligheten att inte ge en handling, upptagning eller upplysning till en part även efter att den person som varit föremål för informationsinhämtning har informerats om användningen av befogenheten för informationsinhämtning. Grunden för att låta bli att ge en handling, upptag-

ning eller upplysning kan förutom att skydda den nationella säkerheten eller liv eller hälsa också vara att skydda privatliv eller sekretessbelagda taktiska och tekniska metoder.

Det föreskrivs särskilt om civila och militära underrättelsemyndigheters skyldighet och rätt att anmäla en brottsmisstanke om ett brott som planeras eller redan har begåtts som har framkommit under användningen av en metod för underrättelseinhämtning till en behörig myndighet (så kallade brandväggsbestämmelser som behandlas nedan i samband med förhållandet mellan civil och militär underrättelseinhämtning och brottsbekämpning). Om en förundersökning inleds i ärendet på grund av en anmälan från den civila eller militära underrättelsemyndigheten, får de aktörer som varit föremål för den kriminella verksamheten i allmänhet kännedom om saken i samband med förundersökningen. I förundersökningslagen föreskrivs om partsoffentlighet vid förundersökning av brott och anmälningar till målsäganden i brott.

Förhållandet mellan civil och militär underrättelseinhämtning och brottsbekämpning

Med kriminalunderrättelseverksamhet för förebyggande av brott stöds förhindrandet av planerad kriminell verksamhet eller avbrytandet av redan påbörjad kriminell verksamhet. Föremålet för kriminalunderrättelseverksamhet som avslöjar brott och kriminalunderrättelseverksamhet som stöder utredning av brott är kriminell verksamhet som redan upphört. Befogenheterna för inhämtande av information vid kriminalunderrättelseverksamhet som avslöjar brott har begränsats att gälla endast landsförräderi- och terroristbrott. Användningen av en metod för underrättelseinhämtning inom civil underrättelseinhämtning får dock fortsättas som hemlig informationsinhämtning för att förebygga eller avslöja landsförräderi-, högförräderi- eller terroristbrott.

I såväl civil och militär underrättelseinhämtning som kriminalunderrättelseverksamhet kan föremålen för informationsinhämtning i synnerhet i fråga om professionell och fortgående organisationsverksamhet vara samtidigt delgärningar som redan avslutats, som pågår eller som planeras i verksamheten. I långsiktig informationsinhämtning avseende professionell och fortgående organisationsverksamhet understryks det behov för skydd och sekretess i informationsinhämtningen som behandlas ovan.

Förebyggande och utredning av brott kan stödas också med öppen informationsinhämtning. I kapitlet om polisens allmänna befogenheter i polislagen föreskrivs bland annat om tillträde och genomsökning vid faro- och skadesituationer. I förundersökningslagen föreskrivs bland annat om förhör och i tvångsmedelslagen även om andra än hemliga tvångsmedel. Underrättelse om omhändertagande av ett föremål, egendom eller en handling för beslag eller kopiering enligt tvångsmedelslagen får dock framskjutas av ett viktigt skäl som har samband med utredningen.

I kapitlet om polisens allmänna befogenheter i polislagen föreskrivs om påverkansbefogenheter för förebyggande av brott. Det kan bland annat röra sig om att skydda hemfrid och offentlig frid, avspärrning av platser och områden, avlägsnande av en person från en plats och gripande för att skydda mot brott och störningar, omhändertagande av farliga föremål och ämnen samt användning av maktmedel för att förhindra ett överhängande brott eller någon annan farlig gärning eller händelse. Teleövervakning omfattar förutom hemlig

informationsinhämtning även tillfälligt förhindrande av användningen av en teleadress eller teleterminalutrustning, som i enlighet med vad som föreskrivs i kapitlet om hemliga metoder för inhämtande av information i polislagen kan användas för att avvärja en allvarlig fara som omedelbart hotar liv eller hälsa. En del av de i tvångsmedelslagen föreskrivna, andra än hemliga tvångsmedlen kan användas för övrigt för att utreda brott, också för att förhindra att den kriminella verksamheten fortsätter.

Föremålet för operativ civil underrättelseinhämtning, operativt civilt kontraspionage och operativt militärt kontraspionage är verksamheten som, om den skulle fortgå, i allmänhet uppfyller rekvisitet för landsförräderi-, högförräderi- eller terroristbrott. Då förutsättningarna för användningen av metoder för underrättelseinhämtning i civil och militär underrättelseinhämtning inte är lika strikt reglerade som förutsättningarna för användningen av metoder för hemlig informationsinhämtning och hemliga tvångsmedel i kriminalunderrättelseverksamhet, och då vissa befogenheter för inhämtande av information finns tillgängliga i civil och militär underrättelseinhämtning men inte i kriminalunderrättelseverksamhet, får civil och militär underrättelseinhämtning dock inte användas för att kringgå regleringen om brottsbekämpningsbefogenheter. Detta gäller såväl civila och militära underrättelsemyndigheters egen verksamhet för att förebygga och avslöja brott som utlämnande av information till en behörig brottsbekämpningsmyndighet. Till exempel får platsspecifik underrättelseinhämtning, som är tillgänglig i civil och militär underrättelseinhämtning, inte användas som "hemlig genomsökning av platser" för att inhämta information för förebyggande, avslöjande eller utredning av brott. Med tanke på tillämpligheten för befogenheter för inhämtande av information är det avgörande om syftet med informationsinhämtningen är att skapa ett informationsunderlag för att skydda den nationella säkerheten och den högsta statsledningens beslutsfattande i samband med det eller att förebygga, avslöja eller utreda vissa enskilda brott.

Om det i samband med civil eller militär underrättelseinhämtning uppkommer en misstanke som överstiger "kan med fog antas/finns skäl att misstänka"-tröskeln om ett brott som planeras eller redan har begåtts, har den civila eller militära underrättelsemyndigheten till uppgift att i princip för det aktuella brottet och inom de ramar som bestämmelserna tillåter välja att antingen börja använda brottsbekämpningsbefogenheterna eller att låta bli att ingripa i det aktuella brottet. Ingetdera slutresultatet av valet förhindrar i sig att även informationsinhämtningen som tangerar det aktuella brottet fortsätter i syfte att skydda den nationella säkerheten, om det aktuella brottet är en del av en större verksamhetshelhet som hotar den nationella säkerheten.

När valet mellan civil och militär underrättelseinhämtning och brottsbekämpning görs, gäller det att beakta förutom intresset gällande skydd av den nationella säkerheten, som i extrema fall förknippas med nationens levnadsmöjligheter, även betydelsen av förebyggande eller utredning av det aktuella brottet för andra allmänna och enskilda intressen. Ett allmänt och enskilt intresse kan betyda bland annat att straffansvaret fullgörs och en eventuell målsägandens förutsättningar att bevaka sin rätt. I samband med statlig och annan organisationsverksamhet kan det i praktiken vara svårt att rikta straffansvaret på en person. Det faktiska fullgörandet av straffansvaret för en person som misstänks för ett brott som redan begåtts kan i samband med statlig verksamhet påverkas av diplomatisk immunitet som personen åtnjuter.

En övergång till användningen av brottsbekämpningsbefogenheter kan i fråga om brott som ingår i civila och militära underrättelsemyndigheters uppgiftsområde innebära de civila och militära underrättelsemyndigheternas egna kriminalunderrättelse- eller påverkansåtgärder för att förhindra eller avslöja det aktuella brottet, eller i fråga om alla brott att det brott som planeras eller redan har begåtts anmäls till den behöriga brottsbekämpningsmyndigheten.

De så kallade brandmursbestämmelserna definierar civila och militära underrättelsemyndigheters skyldighet och rättighet att anmäla en brottsmisstanke till den behöriga brottsbekämpningsmyndigheten. Skyldigheten eller rättigheten att anmäla en brottsmisstanke är i brandväggsbestämmelserna kopplad till brottets allvarlighet (det strängaste föreskrivna straffet för brottet) samt skyldigheten att anmäla en brottsmisstanke om ett brott som redan begåtts också till misstankens styrka ("brott kan antas ha begåtts") och rätten att anmäla ett brott som redan har begåtts också till anmälningens betydelse ("anmälan kan antas vara av synnerlig vikt för utredningen av ett brott").

Viken information som en civil eller militär underrättelsemyndighet är skyldig eller berättigad att lämna ut till den behöriga brottsbekämpningsmyndigheten i samband med anmälan om brott är en skild fråga. Till exempel kan synpunkter gällande skyddandet av underrättelsetjänstemännens och informationskällornas säkerhet och taktiska och tekniska metoder samt begränsningar gällande användning och utlämnande av information som anknyter till internationellt underrättelsesamarbete påverka hur omfattande och detaljerad den information som lämnas ut är. I fråga om internationellt samarbete kan underrättelsesamarbete gällande skydd av den nationella säkerheten, samarbete mellan brottsbekämpande myndigheter gällande kriminalunderrättelseverksamhet och internationell rättshjälp i straffrättsliga ärenden avskiljas från varandra.

Möjligheterna att underlåta att ingripa i ett visst, enskilt brott i samband med civil och militär underrättelseinhämtning bestäms i bestämmelserna om myndighetens uppgifter och uppgifternas prioritet, brandväggsbestämmelserna och enligt vad som föreskrivs om tjänstemannens tjänstgöringsskyldighet (jfr fördröjning med att ingripa i brott och kontrollerade leveranser i kriminalunderrättelseverksamhet). Civila och militära underrättelsemyndigheter har en principiell skyldighet att sköta de civila och militära underrättelseuppdrag som föreskrivs för dem samt uppdrag för förebyggande och avslöjande av brott som har samband med verksamhet som hotar den nationella säkerheten och som äventyrar syftet med det militära försvaret. Myndigheten har både en rättighet och en principiell skyldighet att utöva sina lagstadgade befogenheter för att sköta sina lagstadgade uppgifter. Bestämmelserna om prioritering av myndighetens uppgifter berättigar inte till underlåtenhet att sköta uppgifterna helt och hållet.

Kriminalunderrättelsemyndigheter samt civila och militära underrättelsemyndigheter kan samla in information med hjälp av sina befogenheter för inhämtande av information eller rättigheter att få information, eller från öppna källor.

Förutsättningarna för användning av befogenheten för inhämtande av information och förutsättningarna för användning av den information som fås med hjälp av befogenheten för inhämtande av information ska skiljas från varandra. Syftet med insamlingen av information som fås med hjälp av befogenheten för inhämtande av information, dvs. det

ursprungliga användningsändamålet, bestäms utifrån syftet med informationsinhämtningen, men utöver syftet med informationsinhämtningen ställs för användningen av befogenheten för inhämtande av information även andra villkor. När det gäller förhindrande av kringgående av regleringen om brottsbekämpningsbefogenheter är det däremot inte primärt för vilket ändamål den information som avslöjats oförutsett under användningen av metoden för underrättelseinhämtning används, utan i vilket syfte metoden för underrättelseinhämtning ursprungligen används.

Förutsättningarna för användning av en metod för underrättelseinhämtning i civil eller militär underrättelseinhämtning bestäms utifrån syftet med och föremålen för underrättelseinhämtning, de allmänna förutsättningarna för användning av metoder för underrättelseinhämtning och de särskilda förutsättningarna för användning av metoden för underrättelseinhämtning i fråga.

Om behandlingen av de personuppgifter som kriminalunderrättelsemyndigheter samt civila och militära underrättelsemyndigheter samlar in föreskrivs både i fråga om kriminalunderrättelseverksamhet samt civil och militär underrättelseinhämtning i dataskyddslagen avseende brottmål, lagen om behandling av personuppgifter i polisens verksamhet och i lagen om behandling av personuppgifter inom Försvarsmakten. I både kriminalunderrättelseverksamhet och civil och militär underrättelseinhämtning behandlas förutom personuppgifter även information på fenomennivå. I samband med informationsinhämtning som riktas mot organisationsverksamhet kan även andra sådana uppgifter behandlas, vilka inte direkt eller indirekt anknyter till en identifierad eller identifierbar fysisk person.

Förutsättningarna för behandling av personuppgifter som kriminalunderrättelsemyndigheter samt civila och militära underrättelsemyndigheter samlar in bestäms utifrån de principer som gäller behandling av personuppgifter avsedda i dataskyddslagen avseende brottmål.

Enligt dataskyddslagen avseende brottmål får personuppgifter behandlas endast om det behövs för att en behörig myndighet ska kunna utföra en i lag angiven uppgift (lagenlighetskrav).

Skyddspolisens grundläggande uppgift är att skydda den nationella säkerheten. I deluppgifterna ingår civil underrättelseinhämtning (inhämtande av information för att skydda den nationella säkerheten) samt att förhindra och avslöja sådan verksamhet, sådana förehavanden och sådana brott som kan hota statsskicket och samhällsordningen eller rikets inre eller yttre säkerhet. Enligt lagen om behandling av personuppgifter i polisens verksamhet får Skyddspolisen behandla personuppgifter som behövs för att skydda den nationella säkerheten, för att förhindra, avslöja och utreda verksamhet och förehavanden som hotar stats- och samhällsordningen eller statens säkerhet samt för att förhindra och avslöja brott som hotar stats- och samhällsordningen eller statens säkerhet. Skyddspolisen får, för att sköta sina uppgifter, trots sekretessbestämmelserna lämna ut personuppgifter till andra myndigheter eller till sammanslutningar som sköter offentliga uppgifter samt, om det finns vägande skäl, trots sekretessbestämmelserna i enskilda fall lämna ut personuppgifter till privata sammanslutningar och personer, och om det är nödvändigt för att skyddspolisen ska kunna utföra sina uppgifter.

Försvarsmaktens grundläggande uppgift är att försvara Finland militärt. I deluppgifterna ingår militär underrättelseinhämtning (inhämtande av information om militär verksamhet som riktas mot Finland) samt brottsbekämpning inom Försvarsmakten (förebyggande och avslöjande av brott som anknyter till underrättelseverksamhet som riktar sig mot Finland på det militära försvarets område och till sådan verksamhet som äventyrar syftet med det militära försvaret).

Eftersom de civila och militära underrättelsemyndigheterna inte själva är förundersökningsmyndigheter, är anmälan av brott som anknyter till verksamhet som hotar den nationella säkerheten eller äventyrar det militära försvaret, som avslöjats under användningen av en civil eller militär metod för underrättelseinhämtning och som redan begåtts, till den behöriga förundersökningsmyndigheten det enda sättet som de civila och militära underrättelsemyndigheterna kan slutföra den föreskrivna uppgiften att avslöja brott. Enbart den föreskrivna straffskalan för ett brott ger inte en uttömmande beskrivning av vilken betydelse ett visst avslöjat brott har haft i helheten för verksamhet som hotar den nationella säkerheten eller syftet med det militära försvaret (jfr bestämmelserna om hemligt inhämtande av information för att avslöja ett brott i kapitlet om hemliga metoder för inhämtande av information i polislagen).

Enligt dataskyddslagen avseende brottmål får den personuppgiftsansvarige samla in personuppgifter endast för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandla dem på ett sätt som står i strid med dessa ändamål (ändamålsbegränsning).

I dataskyddslagen avseende brottmål bestämda behandlingsändamålshelheter för uppgifter är bland annat sådan behandling av personuppgifter som utförs av polisen, när uppgifterna behandlas i en sådan polisuppgift som hänför sig till skyddet av den nationella säkerheten, och sådan behandling av personuppgifter som utförs av Försvarsmakten, när uppgifterna behandlas för skötsel av Försvarsmaktens uppgifter.

Syftet med civil underrättelseinhämtning är att inhämta och nyttja information för att den nationella säkerheten ska kunna skyddas och den högsta statsledningens beslutsfattande stödjas samt för att andra myndigheter ska kunna utföra de lagstadgade uppgifter som hänför sig till den nationella säkerheten. Syftet med militär underrättelseinhämtning är att inhämta och behandla information om militär verksamhet som riktar sig mot Finland eller som är av betydelse med tanke på Finlands säkerhetsmiljö eller om en främmande stats verksamhet eller annan sådan verksamhet som allvarligt hotar Finlands försvar eller äventyrar samhällets vitala funktioner för att stöda den högsta statsledningens beslutsfattande och för att Försvarsmakten ska kunna utföra sina uppgifter. Syftet med kriminalunderrättelseverksamhet är att inhämta information för att förebygga, avslöja eller utreda brott.

När civil underrättelseinhämtning (skapandet av ett informationsunderlag för att skydda den nationella säkerheten och den högsta statsledningens beslutsfattande i anslutning till det) samt förebyggande, avslöjande och utredning av brott som hotar den nationella säkerheten är deluppgifter som hör till uppgiftshelheten för skyddande av den nationella säkerheten, blir det aktuellt att bedöma om användningen av information som fås genom en civil underrättelseinhämtningsmetod för att förebygga, avslöja eller utreda brott som hotar den nationella säkerhe-

ten kan anses vara ett användningsändamål som stämmer överens med ändamålet med inhämtandet av informationen.

När militär underrättelseinhämtning (skapandet av ett informationsunderlag för det militära försvaret av Finland och den högsta statsledningens beslutsfattande i anslutning till det) samt förebyggande, avslöjande och utredning av brott som äventyrar syftet med det militära försvaret är deluppgifter som hör till uppgiftshelheten för det militära försvaret av Finland, blir det på motsvararande sätt aktuellt att bedöma om användningen av information som fås genom en militär underrättelseinhämtningsmetod för att förebygga, avslöja eller utreda brott som äventyrar syftet med det militära försvaret kan anses vara ett användningsändamål som stämmer överens med ändamålet med inhämtandet av informationen.

Enligt dataskyddslagen avseende brottmål får personuppgifter behandlas för andra ändamål än sådana som stämmer överens med det ändamål som personuppgifterna insamlats för endast om det föreskrivs om behandlingen i lag (avvikelse från ändamålsbegränsning).

I beslut om användning av en metod för hemligt inhämtande av information och användning av ett hemligt tvångsmedel inom kriminalunderrättelseverksamhet specificeras det brott som man avser förebygga, avslöja eller utreda genom användning av metoden för hemligt inhämtande av information eller det hemliga tvångsmedlet. Om avvikelser från ändamålsbegränsningen för information som fås genom användning av en metod för hemligt inhämtande av information eller ett hemligt tvångsmedel, dvs. användning av informationen för att förebygga, avslöja eller utreda andra brott eller för något annat ändamål som avviker från ändamålet med inhämtande av informationen, föreskrivs i bestämmelserna om användning av överskottsinformation. Med överskottsinformation avses information som inhämtats genom teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter eller teknisk observation i samband med kriminalunderrättelseverksamhet som stöder förebyggande av brott och kriminalunderrättelseverksamhet för avslöjande av brott, och som inte anknyter till ett brott eller avvärjande av fara, eller som gäller något annat brott än det för vars förebyggande och avslöjande tillståndet eller beslutet har getts. I samband med kriminalunderrättelseverksamhet som stöder utredningen av brott avses med överskottsinformation däremot information som fås genom teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter eller teknisk observation och som inte anknyter till ett brott eller som gäller något annat brott än det för vars utredning tillståndet eller beslutet har getts.

Vid utnyttjande i civil och militär underrättelseinhämtning av information på fenomennivå som insamlats i samband med brottsbekämpning är det inte frågan om en situation som omfattas av tillämpningsområdet för bestämmelserna om användning av överskottsinformation. Därutöver får överskottsinformation alltid användas för att inrikta myndighetens verksamhet.

Om användningen av information som inhämtats genom en metod för civil underrättelseinhämtning eller en metod för militär underrättelseinhämtning för att skapa ett informationsunderlag för skyddande av den nationella säkerheten eller det militära försvaret av Finland i syfte att förebygga, avslöja eller förhindra ett brott som anknyter till verksamhet som hotar den nationella säkerheten eller äventyrar det militära försvaret anses vara

ett användningsändamål som stämmer överens med ändamålet med inhämtandet av informationen, tillämpas brandväggsbestämmelserna i detta fall på avvikelser från ändamålsbegränsningen för underrättelseinformation som fås genom att använda metoden för underrättelseinhämtning genom att anmäla en brottsmisstanke om något annat brott än ett brott som gäller verksamhet som hotar den nationella säkerheten eller syftet med det militära försvaret till den behöriga brottsbekämpningsmyndigheten.

Brandväggsbestämmelserna skulle således inte begränsa civila eller militära underrättelsemyndigheters rätt att anmäla en brottsmisstanke om ett brott som gäller verksamhet som hotar den nationella säkerheten eller äventyrar syftet med det militära försvaret till den behöriga brottsbekämpningsmyndigheten.

Lagen om militär underrättelseverksamhet innehåller bestämmelser om användning av information som inte anknyter till ett underrättelseuppdrag. Den faktiska betydelsen av bestämmelserna påverkas av på vilken konkretions- eller abstraktionsnivå underrättelseuppdragen i praktiken specificeras. Ur perspektivet för ändamålet med informationsinhämtningen kan man skilja på militärunderrättelseuppdrag som i princip inte anknyter till straffbar verksamhet och militära kontraspionageuppdrag som i allmänhet anknyter till straffbar verksamhet, även om både militär underrättelseinhämtning och militärt kontraspionage i sig hör till militär verksamhet, såväl när det gäller verksamhet som är föremål för informationsinhämtning som när det gäller egen verksamhet för inhämtande av information. I bestämmelserna om avvikelser från ändamålet med insamling och registrering av uppgifter i lagen om behandlingen av personuppgifter inom Försvarsmakten föreskrivs om behandlingen av uppgifter i säkerhetsdataregistret, som används för att sköta uppgifter som gäller förebyggande och avslöjande av brott, för utförande av militärunderrättelseuppdrag, men inte om behandlingen av uppgifter i militärunderrättelseregistret för att sköta uppgifter som gäller förebyggande och avslöjande av brott.

Enligt dataskyddslagen avseende brottmål ska personuppgifterna som behandlas vara behövliga med hänsyn till ändamålet med behandlingen. Obehövliga personuppgifter ska utplånas utan obefogat dröjsmål. Personuppgifter får inte lagras under en längre tid än vad som behövs med hänsyn till ändamålet med behandlingen (relevanskrav).

Uppgifter som inte behöver utplånas bestäms utifrån bestämmelserna gällande utplåning av information som fås genom användning av befogenheter för inhämtande av information, vilka behandlas ovan i samband med de allmänna förutsättningarna för användning av metoder för underrättelseinhämtning samt principer för civil och militär underrättelseinhämtning. När det gäller civil underrättelseinhämtning är det fråga om information som behövs för att skydda den nationella säkerheten, och när det gäller militär underrättelseinhämtning om information som behövs med tanke på försvaret eller för att skydda den nationella säkerheten. I bestämmelserna möjliggörs även att information som annars ska utplånas kan förvaras och registreras i fråga om civil och militär underrättelseinhämtning i de fall som avses i brandväggsbestämmelserna. Information som behövs för att skydda den nationella säkerheten eller med tanke på försvaret å ena sidan och information som anknyter till de fall som avses i brandväggsbestämmelserna å andra sidan är alltså avskilda från varandra även i fråga om tillämpningen av relevanskravet.

Tolkningen av de brandväggsbestämmelser som ska tillämpas inom civil och militär underrättelseinhämtning försvåras av att bestämmelserna innehåller många element. Bestämmelserna specificerar både rättigheten ("får anmäla") och skyldigheten ("ska anmäla") att anmäla en brottsmisstanke till den behöriga brottsbekämpningsmyndigheten. Även om brandväggsbestämmelserna på det sätt som behandlas ovan skulle tolkas så att de begränsar civila och militära underrättelsemyndigheters rättighet att anmäla en brottsmisstanke till den behöriga brottsbekämpningsmyndigheten endast i fråga om brott som inte hör till civila eller militära underrättelsemyndigheters uppgiftsområde, torde skyldigheten för civila och militära underrättelsemyndigheter att anmäla en brottsmisstanke till den behöriga brottsbekämpningsmyndigheten däremot tolkas att i princip även gälla brott som hör till civila och militära underrättelsemyndigheters uppgiftsområde.

Formuleringarna i brandväggsbestämmelserna lämnar utrymme för tolkning kring huruvida syftet med bestämmelserna är att reglera förutom anmälan av brottsmisstanke på eget initiativ och tillhörande utlämnande av information för brottsbekämpning på eget initiativ även utlämnande av information för brottsbekämpning på begäran (jfr bestämmelserna om användningen av överskottsinformation i kriminalunderrättelseverksamhet). I brandväggsbestämmelserna används i samband med regleringen av rättigheten att utlämna information i fråga om brott som redan har begåtts uttrycket "får anmäla ett begånget brott" och i fråga om brott som är på färde "information som fåtts genom användning av en metod för underrättelseinhämtning får lämnas ut".

Om brandväggsbestämmelserna tolkades så att de endast gäller utlämnande av information på eget initiativ, skulle bestämmelserna om behandling av personuppgifter och inte brandväggsbestämmelserna tillämpas på utlämnande av personuppgifter för brottsbekämpning på begäran. Skyddspolisen får trots sekretessbestämmelserna lämna ut personuppgifter till andra polisenheter bland annat för att förebygga och avslöja brott, för att utreda sådana brott för vilka det i lag föreskrivna strängaste straffet är fängelse, samt för att inrikta polisens verksamhet. Försvarsmakten får trots sekretessbestämmelserna till polisen lämna ut bland annat personuppgifter som behövs för att förebygga, avslöja och utreda brott och föra brott till åtalsprövning.

I samband med riksdagens behandling av lagförslaget om behandling av personuppgifter i polisens verksamhet lades meningen "På utlämnade för brottsbekämpning av uppgifter som har fåtts genom en metod för underrättelseinhämtning ska 5 a kap. 44 § i polislagen iakttas." till i momentet som gäller utlämnande av information till andra polisenheter i bestämmelsen om utlämnande av personuppgifter från Skyddspolisen. Riksdagens förvaltningsutskott ansåg att det fanns skäl att komplettera momentet med en sådan hänvisning till brandväggsbestämmelserna, "varvid det skulle bli helt klart att brandväggsbestämmelsen begränsar rätten att lämna ut personuppgifter när det är fråga om uppgifter som inhämtats genom metoder för underrättelseinhämtning" (FvUB 39/2018 rd). Den tillagda meningen kan tolkas antingen så att brandväggsbestämmelserna ska tillämpas på allt utlämnande av personuppgifter som erhållits genom metoder för underrättelseinhämtning för brottsbekämpning, även sådant som sker på begäran (på utlämnade

för brottsbekämpning av uppgifter som har fåtts genom en metod för underrättelseinhämtning ska brandväggsbestämmelserna *tillämpas*), eller så att brandväggsbestämmelserna ska tillämpas på utlämnande av alla uppgifter, även personuppgifter, som erhållits genom metoder för underrättelseinhämtning, när en brottsmisstanke anmäls på eget initiativ (på utlämnande för brottsbekämpning av uppgifter som har fåtts genom en metod för underrättelseinhämtning ska brandväggsbestämmelserna *iakttas*). Den tillagda meningen torde inte i sig ta ställning till huruvida brandväggsbestämmelserna ska tillämpas endast på brott som inte omfattas av civila och militära underrättelsemyndigheters uppgiftsområde eller också på brott som omfattas av deras uppgiftsområde.

Formuleringarna i brandväggsbestämmelserna ("om det medan en metod för underrättelseinhämtning används framkommer" och "information som fåtts genom användning av en metod för underrättelseinhämtning") lämnar ett visst utrymme för tolkning även kring huruvida de är avsedda att reglera förutom utlämnande för brottsbekämpning av information som civila och militära underrättelsemyndigheter erhållit genom metoder för underrättelseinhämtning även i allmänhet utlämnande för brottsbekämpning av information som civila och militära underrättelsemyndigheter inhämtat eller erhållit på annat sätt i samma eller något annat sammanhang. Det kan vara fråga om till exempel information som en myndighet erhållit genom utövande av sin rätt att få information. Informationen kan också ursprungligen ha erhållits genom användning av en metod för underrättelseinhämtning, men senare ha sparats i ett register, dvs. blivit registeruppgifter. Informationen kan också ha erhållits från en internationell samarbetspartner, som i sin tur kan ha erhållit dem genom användning av en metod för underrättelseinhämtning.

Bakom förhållandet mellan civil och militär underrättelseinhämtning samt brottsbekämpning inverkar också den organisatoriska befogenhetsindelning mellan civila och militära underrättelsemyndigheter samt andra brottsbekämpningsmyndigheter.

Skyddspolisen är såväl myndighet för civil underrättelseinhämtning och civilt kontraspionage som brottsbekämpningsmyndighet gällande föremålen för civil underrättelseinhämtning och civilt kontraspionage. Förutom befogenhet för civil underrättelseinhämtning och civilt kontraspionage har den befogenhet att förebygga och avslöja brott som hotar den nationella säkerheten. Huvudstaben och Försvarsmaktens underrättelsetjänst är såväl myndigheter för militär underrättelseinhämtning och militärt kontraspionage som brottsbekämpningsmyndigheter gällande föremål för militärt kontraspionage. De har befogenhet förutom för militär underrättelseinhämtning och militärt kontraspionage även för förebyggande och avslöjande av brott som anknyter till verksamhet som äventyrar syftet med militärt försvar. I brandväggsbestämmelserna föreskrivs inte om civila eller militära underrättelsemyndigheters rätt att använda information som erhållits genom användning av en metod för underrättelseinhämtning i deras egen verksamhet för att förebygga eller avslöja brott. I synnerhet om det tolkas att brandväggsbestämmelserna gäller endast andra brott än sådana som ingår i civila och militära underrättelsemyndigheters uppgiftsområde skulle en sådan reglering inte vara nödvändig i detta sammanhang. I regeringens proposition med

förslag till lag om militär underrättelseverksamhet betonades dock att samma personer inte ska använda befogenheter enligt lagen om militär underrättelseverksamhet och befogenheter för brottsbekämpning.

Andra brottsbekämpningsmyndigheter har befogenhet att förebygga, avslöja och utreda brott som hör till deras uppgiftsområde. Andra polisenheters än Skyddspolisens uppgiftsområde är allmänt i detta avseende. Utredningen av brott har avskilts från civila och militära underrättelsemyndigheters befogenheter i syfte att trygga en rättvis rättegång. En rättvis rättegång förutsätter att parterna i ett brottmål har tillgång till all sådan information som förundersökningsmyndigheten har inhämtat eller erhållit och som kan antas vara av betydelse i målet. Till exempel skulle restriktioner om användning och vidareutlämnande av information som anknyter till internationellt underrättelsesamarbete vara problematiska i detta avseende.

Behandling av underrättelsetillsyns-ombudsmannens första årsberättelse

Underrättelsetillsynsombudsmannen lämnade sin första berättelse om sin verksamhet (B 14/2020 rd), som gällde år 2019, till riksdagen, riksdagens justitieombudsman och statsrådet 9.6.2020.

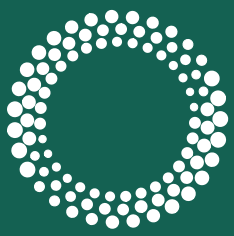
Riksdagen förde en remissdebatt om berättelsen 1.10.2020 och översände ärendet till underrättelsetillsynsutskottet.

De offentliga utlåtanden som de sakkunniga som underrättelsetillsynsutskottet hört med anledning av berättelsen avgett och underrättelsetillsynsombudsmannens kommentarer till dessa har publicerats på riksdagens webbplats. I sakkunnigutlåtandena behandlades bland annat förhållandet mellan övervakaren och den övervakade, tillsynen över användningen av underrättelseinformation i samband med utlåtanden som Skyddspolisen avger till andra myndigheter, tillsynen över Skyddspolisens verksamhet utöver civil underrättelseinhämtning samt offentliggörandet av de övervakningsobservationer som underrättelsetillsynsombudsmannen gjort.

Underrättelsetillsynsutskottet lämnade sitt betänkande om berättelsen (UndUB 1/2020 rd) 15.12.2020. Utskottet konstaterade att tillsynen har varit bra och omfattande. Utskottets övriga centrala observationer gällde avstående från att ge underrättelsemyndigheterna långtgående juridiskt sakkunnigstöd, resurserna för underrättelsetillsynsombudsmannafunktionen, arrangemang gällande underrättelsetillsynsombudsmannen ställföreträdare och diskussioner mellan riksdagens justitieombudsman och underrättelsetillsynsombudsmannen.

Riksdagen godkände 11.2.2021 ett ställningstagande i enlighet med underrättelsetillsynsutskottets betänkande, enligt vilket riksdagen inte hade något att anmärka med anledning av berättelsen.

Riksdagens justitieombudsman tog upp lagtolkningen om de så kallade brandväggsbestämmelserna som framfördes i berättelsen för utredning på eget initiativ och begärde en redogörelse i ärendet av underrättelsetillsynsombudsmannen. Underrättelsetillsynsombudsmannen lämnade sin redogörelse 2.3.2021.



Underrättelsetillsyns-
ombudsman

PB 800, 00531 Helsingfors
tiedusteluvalvonta@om.fi
tiedusteluvalvonta.fi/sv